# IoT Security Guidelines Overview

## Version 1.0

## 26 Apr 2024

### Security Classification: Non-Confidential

### Copyright Notice

### Disclaimer

The GSMA makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice.

### Compliance Notice

The information contain herein is in full compliance with the GSMA Antitrust Compliance Policy.

This Permanent Reference Document has been developed and is maintained by GSMA in accordance with the provisions set out in G SMA AA.34 - Policy and Procedures for Official Documents.

# Table of Contents

# 1 Introduction

## 1.1 Executive Overview

The emergence of the Internet of Things (IoT) has created new service providers who are looking to develop new, innovative, connected products and services. With a year on year increasing deployment base, analysts continue to predict that hundreds of thousands of new IoT services will connect billions of new IoT devices by the end of the decade. This rapid growth of the Internet of Things, combined with private 5G and increasing ability to leverage satellite RAN with 5G, represents a major opportunity for all members of the new ecosystem to expand their service offerings and to increase their customer base.

IoT security issues are a significant inhibitor to the deployment of many new IoT services and, at the same time, the provision of wide area connectivity to an ever-widening variety of IoT services will increase the whole ecosystem's exposure to fraud and attack. There is already much evidence highlighting that attackers are showing ever greater interest in this area.

As these new service providers develop new and innovative services for particular market segments, they may be unaware of the threats their service may face. In some cases, the service provider may not have developed a service that has connected to a communications network or the internet before and they may not have access to the skills and expertise to mitigate the risks posed by enabling internet connectivity within their devices. In contrast, their adversaries understand the technology and security weaknesses, quickly taking advantage if vulnerabilities are exposed. There is a litany of attacks that have resulted in compromised devices. Compromised devices may exfiltrate data, attack other devices, or cause disruption for related or unrelated services.

Whilst many service providers, such as those in automotive, healthcare, consumer electronics and municipal services, may see their particular security requirements as being unique to their market, this is generally not the case. Almost all IoT services are built using endpoint device and service platform components that contain similar technologies to many other communications, computing and IT solutions. In addition to this, the threats these different services face, and the potential solutions to mitigate these threats, are usually very similar, even if the attacker's motivation and the impact of successful security breaches may vary.

The telecommunications industry, which the GSMA represents, has a long history of providing secure products and services to their customers. The provision of secure products and services is as much a process as it is a goal. Vigilance, innovation, responsiveness and continuous improvement are required to ensure the solutions address the threats.

To help ensure that the new IoT services coming to market are secure, the network operators together with their network, service and device equipment partners would like to share their security expertise with service providers who are looking to develop IoT services.

The GSMA has therefore created this set of updated security guidelines for the benefit of service providers who are looking to develop new IoT services.

## 1.2 GSMA IoT Security Guideline Document Set

This document is the first part of a set of GSMA security guideline documents that are intended to help the “Internet of Things” industry establish a common understanding of IoT security issues. The set of guideline documents promotes a methodology for developing secure IoT Services to ensure security best practices are implemented throughout the life cycle of the service. The documents provide recommendations on how to mitigate common security threats and weaknesses within IoT Services.

The structure of the GSMA security guideline document set is shown below. It is recommended that this document, (i.e. the overview document) is read as a primer before reading the supporting documents.

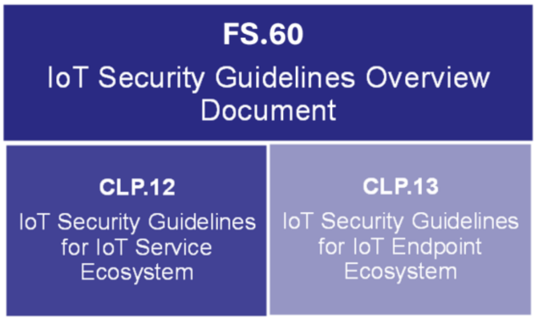
FS.60
IoT Security Guidelines Overview Document
CLP.12
IoT Security Guidelines for IoT Service Ecosystem
CLP.13
IoT Security Guidelines for IoT Endpoint Ecosystem

**Figure 1 - GSMA IoT Security Guidelines Document Structure**

The present document includes top-level security guidelines for Network Operators who intend to provide services to IoT Service Providers to ensure system security and data privacy.

The terms IoT Device and IoT Endpoint are used interchangeably in this document. While many IoT devices are logical end points from a network perspective, the requirements and risk assessment in CLP.13 are intended to be applicable to all IoT devices. The risk assessment will determine the protections necessary for a given IoT device in a given intended deployment scenario.

### 1.2.1 GSMA IoT Security Assessment Checklist

An assessment checklist is provided in document CLP.17 [12]. This document was provided as part of the original IoT Security Guidelines in 2016 to allow self-assessment of products, services and components to the GSMA IoT Security Guidelines.

Since 2016 a number of widely adopted industry baseline security specifications (e.g., ETSI EN 303 645 [25]) and associated assurance specifications (e.g., ETSI TS 103 701 [26]) have been produced. Therefore, while GSMA encourage the use of CLP.17 as a means of initial security baselining internally to a manufacturer or service provider, GSMA recommend the use of EN 303 645 / TS 103 701 or equivalent for the purpose of internationally recognised product security conformity assessments.

## 1.3 Document Purpose

The goal of the Internet of Things Security Guidelines document set is to provide the implementer of an IoT technology or service with a set of design guidelines for building a secure product. To accomplish this task, this document will serve as an overarching model for interpreting what aspects of a technology or service are relevant to the implementer. Once these aspects, or components, are identified, the implementer can evaluate the risks associated with each component and determine how to compensate for them. Each component can be broken down into *sub-components*, where more granular risks will be described. Each risk shall be assigned a priority, to assist the implementer in determining the cost of the attack, as well as the cost of remediation, and the cost, if any, of not addressing the risk.

The scope of this document is limited to recommendations pertaining to the design and implementation of IoT devices, products and services.

Where appropriate this document leverages industry standards such as ETSI EN 303 645 [25], along with wider GSMA industry standards and best practice, to provide a complete set of IoT security guidelines.

It is noted that adherence to national laws and regulations for a particular jurisdiction may, where necessary, require deviation from industry best practice in this document.

The present document replaces previous GSMA IoT Security guideline recommendations contained in CLP.11 and CLP.14.

## 1.4 Intended Audience

The primary audience for this document is:

- IoT Service Providers - enterprises or organisations who are looking to develop new and innovative connected products and services. Some of the many fields IoT Service Providers operate in include smart homes, smart cities, automotive, transport, heath, utilities and consumer electronics.
- IoT Device Manufacturers - providers of IoT Devices to IoT Service Providers to enable IoT Services.
- IoT Developers - build IoT Services on behalf of IoT Service Providers.
- Network Operators who are themselves IoT Service Providers or build IoT Services on behalf of IoT Service Providers.
- Regulators – National or Regional jurisdictions who are looking to leverage industry best practice for IoT and ensure that any regulations minimise market fragmentation.
- Testing – Manufacturer, operator or 3rd party labs who test IoT devices, products and services.

## 1.5 Definitions

| Term | Description |
|---|---|
| Access Point Name | Identifier of a network connection point to which an endpoint device attaches. They are associated with different service types, and in many cases are configured per network operator. |
| Attacker | A hacker, threat agent, threat actor, fraudster or other malicious threat to an IoT device, product or service, typically with the intent of retrieving, destroying, restricting or falsifying information. This threat could come from an individual criminal, organised crime, terrorism, hostile governments and their agencies, |

| Term | Description |
|---|---|
| | industrial espionage, hacking groups, political activists, ‘hobbyist’ hackers, researchers, as well as unintentional security and privacy breaches. |
| Cloud | A network of remote servers on the internet or at network edge that host, store, manage, and process applications and their data. |
| Complex Endpoint | This IoT device model has a persistent connection to a back-end server over a long-distance communications link such as cellular, satellite, or a hardwired connection such as Ethernet. See CLP.13 [4] for further information. |
| Components | Refers to the components contained in documents CLP.12 [3] and CLP.13 [4] |
| Edge Cloud | A set of local cloud resources, located at the edge of the network close to the IoT device enabling low delay, aggregation or localised high bandwidth processing. |
| Embedded SIM | A SIM which is not intended to be removed or replaced in the device, and enables the secure changing of profiles as per GSMA SGP.01 [2] and SGP.31[22]. |
| Endpoint | A generic term for a lightweight endpoint, complex endpoint, gateway or other connected devices. See CLP.13 [4]for further information. |
| Endpoint Ecosystem | Any configuration of low complexity devices, rich devices, and gateways that connect the physical world to the digital world in novel ways. See section 4.2 for further information. |
| Internet of Things | The Internet of Things (IoT) describes the coordination of multiple machines, devices and appliances connected to the Internet or to a private mobile network (e.g. private 5G), through multiple networks. These devices include everyday objects such as tablets and consumer electronics, and other machines such as vehicles, monitors and sensors equipped with communication capabilities that allow them to send and receive data. |
| IoT Product | A device placed on the market, made up of one or more components. The device may directly offer one or more IoT services or may be integrated (e.g., an IoT sensor) into a wider IoT service. IoT products may be themselves integrated into other larger devices (e.g., washing machines or industrial systems) to provide an IoT capability in a larger integrated product. |
| IoT SAFE | IoT SIM Applet for Secure End-2-End communication |
| IoT Service | Any computer program that leverages data from IoT devices to perform the service. |
| IoT Service Provider | Enterprises or organisations who are looking to develop new and innovative connected products and services. |
| Network Operator | The operator of the communication network that connects the IoT endpoint device to the IoT service ecosystem. |
| Organisational Root of Trust | A set of cryptographic policies and procedures that govern how identities, applications, and communications can and should be cryptographically secured. |
| Recommendations | Refers to the recommendations contained in documents CLP.12 [3] and CLP.13 [4] |
| Risk | Refers to the risks contained in documents CLP.12 [3] and CLP.13 [4] |
| Security Tasks | Refers to the security tasks contained in documents CLP.12 [3] and CLP.13 [4] |
| Service Access Point | A point of entry into an IoT Service’s back-end infrastructure via a communications network. |

| Term | Description |
|---|---|
| IoT Service Ecosystem | The set of services, platforms, protocols, and other technologies required to provide capabilities and collect data from endpoints deployed in the field. |
| Subscriber Identity Module (SIM) | The smart card used by a mobile network to authenticate devices for connection to the mobile network and access to network services. |
| UICC | A secure element platform specified in ETSI TS 102 221 [23] that can support multiple standardised network or service authentication applications in cryptographically separated security domains. It may be embodied in embedded form factors specified in ETSI TS 102 671 [24]. |

## 1.6 Abbreviations

| Term | Description |
|---|---|
| 3GPP | 3rd Generation Project Partnership |
| ABP | Activation By Personalisation |
| AES | Advanced Encryption Standard |
| AI | Artificial Intelligence |
| APDU | Application Protocol Data Units |
| API | Application Program Interface |
| APN | Access Point Name |
| BLE | Bluetooth Low Energy |
| CANbus | Controller Area Network bus |
| CAPIF | Common API Framework |
| CD-ROM | Compact Disc - Read Only Memory |
| CEIR | Central Equipment Identity Register |
| CERT | Computer Emergency Response Team |
| CLP | GSMA's Connected Living Programme |
| CPU | Central Processing Unit |
| CRA | Cyber Resilience Act |
| CVD | Coordinated Vulnerability Disclosure |
| DDoS | Distributed Denial of Service |
| DoS | Denial of Service |
| DPIA | Data Protection Impact Assessment |
| DPPDD | Data Protection and Privacy by Design and Default |
| DVD | Digital Video Disc |
| EAB | Extended Access Barring |
| EAP | Extensible Authentication Protocol |
| ECU | Electronic Control Unit |
| EEA | EPS Encryption Algorithm |
| EEPROM | Electrically Erasable Programmable Read-Only Memory |
| EIA | EPS Integrity Algorithm |

| Term | Description |
|---|---|
| EIR | Equipment Identity Register |
| EPS | Evolved Packet System |
| eSIM | Embedded SIM |
| ETSI | European Telecommunications Standards Institute |
| EU | European Union |
| eUICC | Embedded UICC |
| FASG | Fraud and Security Group |
| FIPS | Federal Information Processing Standards |
| GAA | Generic Authentication Architecture |
| GNSS | Global Navigation Satellite System |
| GBA | Generic Bootstrapping Architecture |
| GDPR | General Data Protection Regulation |
| GEA | GPRS Encryption Algorithm |
| GIA | GPRS Integrity Algorithm |
| GNSS | Global Navigation Satellite System |
| GPRS | General Packet Radio Service |
| GPS | Global Positioning System |
| GPSI | Generic Public Subscription Identifier |
| GSMA | GSM Association |
| GUI | Graphic User Interface |
| HIPAA | Health Insurance Portability and Accountability Act |
| HBRT | Hardware Based Root of Trust. |
| HRM | Heart Rate Monitor |
| HSS | Home Subscriber Server |
| ICCID | Integrated Circuit Card Identifier |
| ICO | Information Commissioner’s Office |
| IMEI | International Mobile Equipment Identity |
| IMSI | International Mobile Subscriber Identity |
| IoT | Internet of Things |
| IP | Internet Protocol |
| IT | Information Technology |
| LiPo | Lithium Polymer |
| LPWA | Low Power Wide Area |
| LTE-M | Long Term Evolution for Machines |
| MCU | MicroController Unit |
| MSISDN | Mobile Station International Subscriber Directory Number |
| NB-IoT | Narrowband-Internet of Things |
| NESAS | Network Equipment Security Assurance Scheme |

| Term | Description |
|---|---|
| NIST | National Institute of Standards and Technology |
| NVRAM | Non-Volatile Random Access Memory |
| OBD | On Board Diagnostics |
| OCTAVE | Operationally Critical Threat, Asset, and Vulnerability Evaluation |
| OMA | Open Mobile Alliance |
| OTA | Over The Air |
| OTAA | Over The Air Activation |
| PDR | Privacy Design Recommendation |
| PEI | Permanent Equipment Identifier |
| PIA | Privacy Impact Assessment |
| PII | Personally Identifiable Information |
| PP | Privacy Principle |
| RAN | Radio Access Network |
| RAM | Random Access Memory |
| RCS | Rich Communication Services |
| RSP | Remote SIM Provisioning |
| SAS | Security Accreditation Scheme |
| SIM | Subscriber Identity Module |
| SMS | Short message Service |
| SUPI | Subscription Permanent Identifier |
| TCB | Trusted Compute Base |
| TPM | Trusted Platform Module (except section 12) |
| TPM | Tyre Pressure Monitor (section 12 only) |
| TVRA | Threat Vulnerability Risk Analysis |
| UDM | Unified Data Management |
| UICC | Universal Integrated Circuit Card |
| USSD | Unstructured Supplementary Service Data |
| UK | United Kingdom |
| V2I | Vehicle to Infrastructure |
| V2V | Vehicle to Vehicle |
| WAN | Wide Area Network |

## 1.7 References

| Ref | Doc Number | Title |
|---|---|---|
| [1] | n/a | “The Mobile Economy 2023” https://www.gsma.com/mobileeconomy/ |
| [2] | SGP.01 | “Embedded SIM Remote Provisioning Architecture”<br>https://www.gsma.com/esim/resources/sgp-01-v4-1-pdf/ |
| [3] | CLP.12 | IoT Security Guidelines for IoT Service Ecosystem<br>https://www.gsma.com/iot/future-iot-networks/iot-security-guidelines/ |

| Ref | Doc Number | Title |
|---|---|---|
| [4] | CLP.13 | IoT Security Guidelines for IoT Endpoint Ecosystem<br>https://www.gsma.com/iot/future-iot-networks/iot-security-guidelines/ |
| [5] | n/a | NIST Risk Management Framework<br>http://csrc.nist.gov/groups/SMA/fisma/framework.html |
| [6] | CMU/SEI-2007-TR-012 | Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process<br>http://www.cert.org/resilience/products-services/octave/ |
| [7] | 3GPP<br>TS 33.220 | Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA) https://www.3gpp.org/dynareport/33220.htm |
| [8] | RFC 4186 | Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)<br>https://www.rfc-editor.org/rfc/rfc4186 |
| [9] | n/a | Conducting privacy impact assessments code of practice<br>https://ico.org.uk/media/about-the-ico/consultations/2052/draft-conducting-privacy-impact-assessments-code-of-practice.pdf |
| [10] | n/a | Open Mobile Alliance<br>https://omaspecworks.org/ |
| [11] | n/a | oneM2M Specifications<br>http://www.onem2m.org/ |
| [12] | CLP.17 | GSMA IoT Security Assessment Checklist<br>https://www.gsma.com/iot/iot-security-assessment/ |
| [13] | n/a | 65% of the World's Population Will Have Its Personal Data Covered Under Modern Privacy Regulations<br>https://www.gartner.com/en/newsroom/press-releases/2020-09-14-gartner-says-by-2023--65--of-the-world-s-population-w |
| [14] | n/a | Testing our Trust: Consumers and the Internet of Things 2017 Review' Consumers International<br>https://www.consumersinternational.org/media/154746/iot2017review-2nded.pdf |
| [15] | n/a | 'People are really worried about IoT data privacy and security', Networked World<br>https://www.networkworld.com/article/3267065/internet-of-things/people-are-really-worried-about-iot-data-privacy-and-securityand-they-should-be.html |
| [16] | n/a | Regulation (EU) 2016/679 (GDPR)<br>https://eur-lex.europa.eu/eli/reg/2016/679/oj |
| [17] | n/a | Privacy by Design - The 7 Foundational Principles - Ann Cavoukian.<br>https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-implement-7found-principles.pdf |
| [18] | n/a | Convention 108 + Convention for the protection of individuals with regard to the processing of personal data<br>https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1 |

| Ref | Doc Number | Title |
|---|---|---|
| [19] | n/a | Indian Ministry of Electronics & Information Technology Personal Data Protection Bill<br>https://www.meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill%2C2018_0.pdf |
| [20] | n/a | UK Data Protection Act<br>https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted |
| [21] | GSMA IoT.04 | Common Implementation Guide to Using the SIM as a 'Root of Trust' to Secure IoT Applications<br>https://www.gsma.com/iot/iot-safe/ |
| [22] | GSMA SGP.31 | eSIM IoT Architecture and Requirements<br>https://www.gsma.com/esim/resources/sgp-31-esim-iot-architecture-and-requirements/ |
| [23] | ETSI TS 102 221 | Smart Cards; UICC-Terminal interface; Physical and logical characteristics<br>https://www.etsi.org/standards |
| [24] | ETSI TS 102 671 | Smart Cards; Machine to Machine UICC; Physical and logical characteristics<br>https://www.etsi.org/standards |
| [25] | ETSI EN 303 645 | CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements<br>https://www.etsi.org/standards |
| [26] | ETSI TS 103 701 | CYBER; Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements<br>https://www.etsi.org/standards |
| [27] | ETSI TR 103 838 | Cyber Security; Guide to Coordinated Vulnerability Disclosure<br>https://www.etsi.org/standards |
| [28] | n/a | GSMA CVD Programme<br>https://www.gsma.com/security/gsma-coordinated-vulnerability-disclosure-programme/ |
| [29] | ETSI TR 103 621 | Guide to Cyber Security for Consumer Internet of Things<br>https://www.etsi.org/standards |
| [30] | n/a | EU Right to Repair: Making repair easier for consumers.<br>https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_23_1794/IP_23_1794_EN.pdf |
| [31] | n/a | UK ICO Data Protection Impact Assessments (PIAs)<br>https://ico.org.uk/for-organisations/law-enforcement/guide-to-le-processing/accountability-and-governance/data-protection-impact-assessments. |
| [32] | n/a | Wassenaar Export Control Arrangement<br>https://en.wikipedia.org/wiki/Wassenaar_Arrangement |
| [33] | GSMA CLP.03 | IoT Device Connection Efficiency Guidelines <LINK> |
| [34] | GSMA FS.04 | Security Accreditation Scheme for UICC Production <LINK> |
| [35] | GSMA FS.13 | GSMA NESAS Overview <LINK> |
| [36] | GSMA IoT.04 | Common Implementation Guide to Using the SIM as a |

| Ref | Doc Number | Title |
|---|---|---|
| | | 'Root of Trust' to Secure IoT Applications. <LINK> |
| [37] | n/a | GSMA Rich Messaging Services (RCS) <LINK> |
| [38] | n/a | GSMA Mobile IoT Deployment Guide – October 2022 <LINK> |
| [39] | 3GPP<br>TS 33.122 | Security aspects of Common API Framework (CAPIF) <LINK> |
| [40] | GSMA FS.31 | GSMA Baseline Security Controls <LINK> |
| [41] | ETSI TS 102 165 | Threat Vulnerability Risk Analysis (TVRA) |
| [42] | n/a | UK Security Requirements for Relevant Connectable Products 2023 <LINK> |
| [43] | n/a | EU Cyber Resilience Act (CRA) <LINK> |
| [44] | n/a | ISO/IEC 62443 Security for industrial automation and control systems <LINK> |

# 2 The Security Challenges Created by the Internet of Things

## 2.1 General

The internet of things has expanded rapidly beyond the initial concepts of Industry 4.0 into a broad collection devices, products and services that are now critical to most people on the planet's daily lives. From wearables to industrial process sensors, to environment monitoring and supply chain tracking IoT devices are now omni-present in society.

These devices and associated services collect and process vast amounts of either personal or security sensitive data. Many devices operate in constrained environments (limited size, transmission bandwidth, power, human interfaces, low security locations) and may have little or no direct human supervision. Many IoT devices may form part of safety systems or are part of critical national infrastructure.

Similarly, many devices are integrated into building or transport systems which cannot be readily replaced, or hardware upgraded over their lifetimes. Furthermore, whether integrated or not most IoT devices associated services demand a relatively high device volumes, with low price points, which limits the inclusion of many state-of-the-art security platform features that are included in 2000-dollar smartphones and behave as intended.

However, baseline security features need to be provided in all IoT devices, products and services as detailed in these GSMA IoT guidelines, to ensure that all IoT devices, products and services adequately protect sensitive data.

From a network perspective IoT devices significantly increase the number of end points but in general have much lower data rate demands than smart phones. Similarly, the sheer volume of IoT devices represent a Distributed Denial of Service (DDOS) attack on networks and services. Given that IoT devices are frequently attached to critical infrastructure or safety critical systems, simply kicking them off the network as would be possible for a malicious smart phone is less practical.

From a user perspective, the lower direct user interaction with most IoT devices (except wearables) compared to smartphones means that users are less aware or concerned of potential developing security issues. This also implies that users need to be provided with convenient and secure management tools to control and pre-configure their fleet of devices, rather than be expected to react immediately to notifications during operation of any device. Patching of IoT devices (especially constrained devices) can be more difficult than for smart phones or tablets.

As a minimum, all consumer IoT devices, products and services should meet the requirements set out in ETSI EN 303 645 [25] in order to provide a minimum-security baseline. While EN 303 645 isn’t specifically aimed at non consumer devices, since non consumer devices present and are exposed to many of the same risks as consumer devices, EN 303 645 should be considered good starting point for all IoT devices on top of which any industrial or sector specific requirements can be applied. ETSI provide further background advice to support the implementing EN 303 645 requirements in ETSI TR 103 621 [29]. For industrial IoT devices, the use of ISO/IEC 62443 [44] may also be considered.

While historically compliance with standards such as EN 303 645 have been optional, countries are increasingly looking to mandate compliance with specific technical standards (or requirements derived from those standards) for all IoT devices placed on the market. Examples include the 2023 UK Security Requirements for Relevant Connectable Products Regulations [42], with many others in the pipeline such as EU Cyber Resilience Act (CRA) [43].

To secure IoT effectively it is necessary to address the following challenges:

- Availability: Ensuring constant secure connectivity between IoT devices and their respective services.
- Identity: Authenticating IoT devices, services, integrity and the customer or end-user operating the IoT device.
- Privacy: Ensure that privacy sensitive information or security sensitive data (in case of industrial systems) is protected both in the endpoint devices and in transit.
- Security: Ensuring that device, service and overall IoT system can, where necessary, have their integrity attested, verified, and audited.

## 2.2 The Availability Challenge

IoT devices must be able to securely communicate with each other, end-users, and back-end services. To accomplish this, 5G technologies such as NB-IoT and LTE-M are being deployed allowing persistent connectivity for low power devices. This dovetails well with the challenge of ubiquitous Internet access for the modern world. For this to succeed, several questions must be answered:

- How can Low Power Wide Area (LPWA) networks (e.g. NB-IoT and LTE-M) be deployed and operated with a similar level of security to traditional cellular systems?
- How can multiple mobile operators support the same level of network security as IoT endpoints migrate across network boundaries?
- How can network trust be forwarded to capillary endpoints that rely on gateway endpoints for communication?

- How can the power constraints of lightweight endpoints be addressed in secure communications environments?

## 2.3 The Identity Challenge

For an IoT device to securely function within an IoT product or service ecosystem (either as a single endpoint or one of multiple IoT devices forming an endpoint), it must be capable of mutually identifying itself to its peers and services. This critical and fundamental aspect of IoT technology ensures that IoT devices, services and peers can guarantee to what – and to whom – data is being delivered or received. Access to information and services isn't the only issue directly tied to identity. Where applicable:

- The user operating the device needs to be strongly associated with the device's identity.
- Services and peers need to be able verify the identity of the end-user by verifying the identity of the \IoT device.
- Device endpoint security technology needs to be capable of securely authenticating peers and services.
- IoT devices, services and peers need to be able to detect and prevent any attempt to impersonate authorised services and peers.
- The identity of a device needs to be trusted and secured from tampering or manipulation.
- The IoT device and network need to ensure that only authorised IoT services are permitted to access the IoT device.

## 2.4 The Privacy Challenge

Since GDPR [16] or equivalent local legislation, privacy can no longer be seen as an add-on to existing products and services. Privacy must be designed into products from the ground up, to ensure that every action is authorised and every identity is verified while guaranteeing that these actions and the associated meta-data are not exposed to unauthorised parties. This can only be achieved by defining an appropriate risk-based security architecture for a product or service and is usually exceptionally difficult and prohibitively expensive to perform retroactively. Annex A of this document contains a set of informative privacy recommendations.

Medical devices, automotive solutions, industrial control systems, home automation, building and security systems, and more, all directly impact human physical lives. It is the duty of the engineers to uphold these products and services to the highest level of assurance possible, to reduce the potential for physical harm as well as the exposure of privacy relevant data.

Many IoT devices do not generate, process, transmit or store personal data directly (e.g. most industrial control systems). However, the data generated by such devices is often security sensitive and requires security controls equivalent to that for protecting privacy sensitive information. Additionally, while some consumer IoT devices don't directly handle privacy sensitive information either, the association of a device with a user or the location of the device may result in a privacy risk to the user and therefore still require privacy protection to be applied in such devices.

Manufacturers and service designers need to apply a secure by default approach to all data generated, processed, stored or transmitted by IoT devices unless a risk assessment has been undertaken to confirm that a lower level of protection may be applied. However, other requirements may need to take precedence over the default privacy by design approach (e.g. accessibility requirements for assistance devices or the need to perform traffic filtering).

Therefore, IoT technologies need to be designed to ensure where appropriate that:

- The identity of an IoT device is not exposed to unauthorised users or 3rd parties.
- Unique IoT device or IoT service identifiers do not allow an end-user or IoT device to be physically monitored or tracked by unauthorised parties.
- Data emanating from an IoT device or IoT service indicative of or directly associated with physical end-user attributes such as location, action, or a state, such as sleeping or awake is protected.
- Confidentiality and integrity mechanisms employed are of sufficient security strength.
- Where practical algorithm agility has been considered to allow fixing any weaknesses that may be identified after the product or service is placed on the market.
- The product or service securely stores and handles user-specific Personally Identifiable Information (PII).
- The end-user can control the storage or use of PII in the IoT service or product, including the right to be forgotten and delete all data.
- IoT device security keys used to secure data, communicate with the IoT Service to secure the data be refreshed.
- As per ETSI EN 303 645 [25], the IoT device does not use universal default passwords and any endpoint or service passwords can be changed by the user or IoT service administrator (as appropriate).
- The IoT device provides the ability for the user to disassociate the IoT device from a service and return it back to factory state removing all personal data.

## 2.5 The Security Challenge

While Internet security has drastically improved over the past several decades, IoT security frequently lags behind wider computer or internet security and often repeats many of the same previously addressed historic weaknesses. These gaps have been most evident in embedded IoT systems and in IoT cloud services - the two primary components in IoT technology.

For IoT to avoid exposing massive groups of users and physical systems to risk, information security practices must be enforced on both IoT devices and IoT services. Where appropriate:

- Security best practices need to be incorporated into the product or service at the by design
- Security of both IoT devices and services needs to be considered and addressed throughout their entire lifecycle included end of use or re-use by different users. (see section 4)
- Is appropriate risk-based application security (e.g. end to end) applied to both services and applications running on the embedded system.

- A Trusted Computing Base (TCB) implemented in both the IoT devices and the service ecosystem.
- The TCB needs to enforce self-verification of application images and services
- Can IoT devices and IoT services detect if there is an anomaly in their configuration or applications?
- Managed IoT endpoint devices are monitored for anomalies indicative of malicious behaviour.
- Authentication and identity are tied to the product or service security processes.
- For managed IoT endpoints devices or services to have an incident response plan defined for detected anomalies indicative of a compromise.
- Services and resources are segmented to ensure a compromise can be contained quickly and effectively.
- All services and applications run with least privilege.
- Consider how are services and resources restored after a compromise?
- Consider how anomaly and compromise detection can be applied at a system component level.
- Provide an easy to access means for customers to report security concerns.
- Provide a Coordinated Vulnerability Disclosure (CVD) scheme [27],[28] for security researchers to report any vulnerabilities they find in IoT endpoints or services.
- IoT devices can be updated or patched to remove vulnerabilities.

# 3 The Mobile Solution

## 3.1 General

While there has been a myriad of technologies that offer connectivity solutions for IoT, none continue to shape the future of IoT better than mobile networks. Mobile networks offered the first wireless services to consumers and industry over thirty years ago, and have been building reliable, available, secure, and cost-effective services ever since. Mobile networks have evolved to offer IoT specific capabilities and services that are optimised for IoT devices and services. Network identity has been a challenge that has spawned numerous standards, device technologies, protocols and analytics models. Privacy and security are constant concerns of the mobile industry, who have worked to decrease the potential for abuses, identity theft, and fraud in all mobile technology.

The mobile industry is offering standards based, licensed, Low-Power Wire-Area (LPWA), 5G wireless network technologies such as NB-IoT and LTE-M to cover the needs of IoT applications and services. These LPWA network technologies offer the same (and in many cases increased) wide area, wireless connectivity of traditional mobile networks at a fraction of the power required to communicate effectively. Many network operators have deployed LPWA services such that NB-IoT and LTE-M are becoming the de facto standards for LPWA network deployment.

Further information regarding NB-IoT and LTE-M network deployment in worldwide regions can be found on the GSMA website: https://www.gsma.com/iot/deployment-map/

## 3.2 Addressing the Challenge of Availability

According to the GSMA's "The Mobile Economy 2023" report [1]:

- By the end of 2022, 68% of the world’s population had a mobile subscription – a total of 5.4 billion unique subscribers. By 2030, almost three quarters of the world’s population – or 6.3 billion people – will subscribe to mobile services.
- The shift to mobile broadband networks and smartphones continues to gain momentum. Mobile broadband connections (smartphones) accounted for 76% of total connections in 2022 – a figure that will be close to 92% of the connections base by 2030. The proportion of 5G connections alone is forecast to increase four-fold from 12% in 2022 to 54% by the end of the decade.
- An additional 1.4 billion mobile broadband connections are forecast between 2022 and 2030, with the proportion of the total rising to 92%. With the migration to 5G, 4G connection numbers are expected to decrease from 60% in 2022 to 36% in 2030. In 2022, 2G is no longer the dominant technology in terms of connections. Excepting Sub-Saharan African where 3G dominates, in 2022 4G was the dominant technology.
- The number of IoT connections is large, totalling around 5.3 billion connections by 2030, from a base of 2.5 billion in 2022.

## 3.3 Addressing the Challenge of Identity

Identity management has been a challenge for decades and has strengthened the mobile industry’s standards and technology offerings significantly. While the mobile industry is typically associated with the removable SIM card, the GSMA has created a SIM based solution called the ‘eSIM IoT Architecture and Requirements” [22] which is intended for IoT to enable deeper component level integration into IoT devices, reduced production costs and the management of connectivity via Over-The-Air (OTA) platforms to enable the connectivity of the IoT devices for their whole lifetime.

Identity technologies, such as the embedded SIM, are designed as trust anchors that integrate security by default. They are manufactured to withstand attacks such as:

- Glitching
- Side-channel analysis
- Passive data interception
- Physical tampering
- Identity theft

An excellent advancement to this already security hardened technology is that new generations of these trust anchors incorporate an important addition to the IoT landscape. These technologies are dual use. They aren’t simply be used to verify the security of the network, they are also capable of securing application communications and the application itself, similar to traditional computing trust anchors.

This dual use capability can be further augmented by the integration of mobile industry security specifications such as those provided by 3GPP GBA [7], OMA [10], oneM2M [11] and others. These technologies help to securely provision devices in the field, securely enable over-the-air firmware updates, and manage device capabilities and identity.

These technologies, when used together, can ease the currently complex engineering processes and combine it into one simple component. Instead of application engineers building complex technologies that they themselves must manage, the network operator, who already manages the network identity, can perform this on behalf of the application.

This not only reduces the engineering complexity, but the business's daily management requirements.

### 3.4 Addressing the Challenge of Privacy and Security

Along with the capabilities of the SIM, the mobile industry has developed resilient protocols, processes, and monitoring systems to enable security and reduce the potential for fraud and other malicious activities. For example, 3G, 4G and 5G technologies use mutual authentication to verify the identity of the IoT devices and the network. This process helps ensure that adversaries are unable to intercept communications.

Furthermore, network technology can be secured using the SIM and technologies such as GBA [7] or EAP-SIM [8]. By using these technologies, the SIM can be provisioned with a session security key to be used in communications with application network peers over well-known protocols. This process can diminish the potential for adversaries to manipulate the application protocol to compromise the devices or service. Thus, it is possible to secure both the network and the application with this model.

In addition, all IoT devices need to include a hardware-based root of trust (HBRT) which is used to attest both the hardware and software at IoT device boot and can be used to validate and authenticate firmware or other endpoint software updates. The HBRT can be integrated with or leverage capabilities of the eSIM [2].

# 4 The IoT Model

### 4.1 General

Figure 2 illustrates the standard IoT model used throughout these documents and depicts components of the service and endpoint ecosystems. Each component is composed of sub-components, which are detailed in a document that focuses solely on the primary component. For example, the IoT endpoint device component, and its respective risks, are outlined in the Endpoint Ecosystem document [4] provided within this document set and the service components are outlined in the Service Ecosystem document [3].

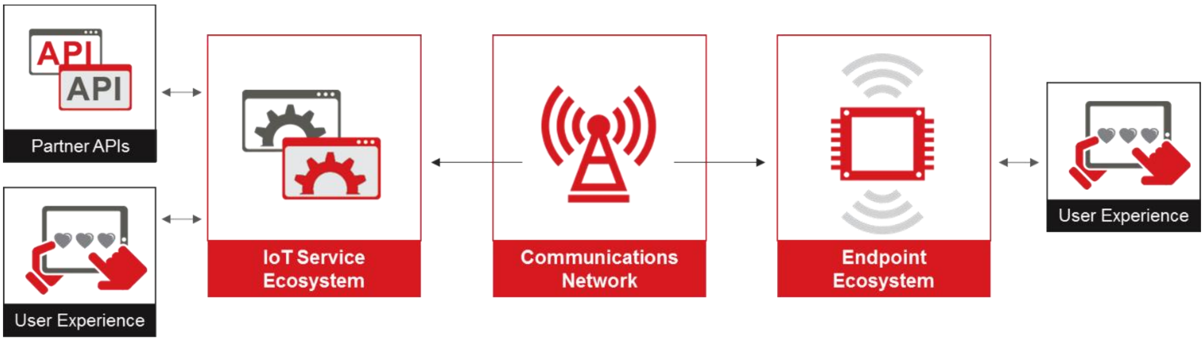

**Figure 2 - Example IoT Model**

In almost all modern IoT service or product models, this diagram defines the primary components that are required when deploying a production-ready technology.

Communications network components are inherent to IoT and, for the purposes of this model, provide the connection between the two ecosystems with each 'end' of the communication link discussed within the appropriate Endpoint Ecosystem and Service Ecosystem document.

Specific network security guideline recommendations for network operators can be found in sections 7 and 8.

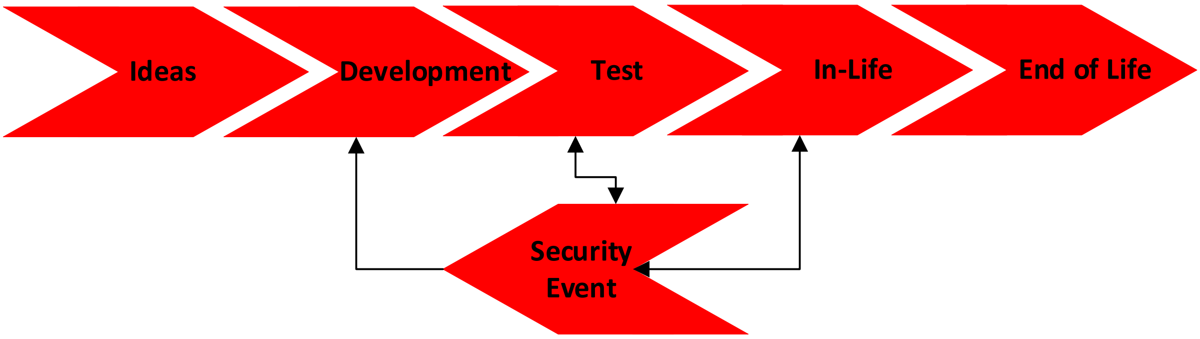

**Figure 3 – IoT Life Cycle Model**

As discussed in section 2.5, security and privacy need to be considered throughout the whole lifecycle of an IoT product or service. Figure 3 represents a simplified lifecycle of a typical IoT product or service. Security events (e.g. vulnerabilities are reported through the manufacturer's CVD scheme), may be frequent throughout the lifecycle of a product and may occur at any time. Manufacturers and service operators need processes in place to handle such events and provide patches in a timely manner. Similarly, IoT manufacturers and service operators need to clearly identify during product development who is responsible for support of what, within their product architectures and supply chains.

The frequently overlooked end of life stage needs to be considered to ensure that any IoT devices do not pose a security risk after the user has finished with them (e.g. data can be stolen during the device recycling processes). Similarly with increasing legislation in EU and globally on right to repair [30], and consumers increasingly reselling devices on online marketplaces, device security and privacy needs to be also considered in these scenarios.

## 4.2 Service Ecosystem

The Service Ecosystem represents the set of services, platforms, protocols, and other technologies required to process and collect data from IoT devices deployed in the field. This ecosystem typically processes input data into output data from IoT devices and stores them within its server environment or forwards the data to other devices in a system to perform actions (e.g. actuators). This data can be rendered to the user by handing elegant visual depictions of the data to various user interfaces. This data, often in the form of metrics, parameters or commands, can also be handed off to authorised third parties via an API (e.g. oneM2M [11]) originating at the service infrastructure, which is commonly how IoT Service Providers monetise the service.

The Service Ecosystem security guidelines to be used in conjunction with the process described in this overview document can be found in CLP.12 IoT Security Guidelines for IoT Service Ecosystem [3]

### 4.3 IoT Device Endpoint Ecosystem

The Endpoint Ecosystem [4] consists of low complexity devices, rich devices and gateways that connect the physical world to the digital world in via several types of wired and wireless networks. Examples of common IoT devices are motion sensors, digital door-locks, automotive telematics systems, sensor-driven industrial control systems, and more. IoT endpoint devices gather metrics from the physical environment around them and push that data in different formats via a capillary or cellular network to the service ecosystem, often receiving instructions or actions in response. They may also include rich user interfaces that render data obtained either through the IoT device itself, or from the service ecosystem.

It is essential that the endpoint ecosystem IoT devices support secure remote management capabilities for owners of endpoints deployed on the field and they include per device unique credentials supported by HRBT (e.g., UICC or TPM).

The Endpoint Ecosystem security guidelines to be used in conjunction with the process described in this overview document can be found in CLP.13 IoT Security Guidelines for IoT Endpoint Ecosystem [4].

### 4.4 Design Agility Considerations

During the In-Life stage of a product's lifecycle in Figure 3, products will be subject to changes in the security landscape or threat environment within which the product is used. These could be industry wide compromise of an algorithm or the eventual arrival of a cryptographically relevant quantum computer. It is therefore important to consider during the product development phase and during any risk assessments (as per section 5), how the product may need to involve overtime from a security perspective.

Where feasible, IoT products should include security and cryptographic agility such that algorithms or other security critical features can if necessary be securely updated during the product lifecycle. This is especially important for long life or hard to replace products. Clearly this may not be practical for all products (e.g. low cost, power or size constrained devices).

Similarly, where a product is expected to be hard to replace (e.g., those integrated into buildings), designers should consider the risks and implications of a low security agility device needing to co-exist with other higher security sensitivity devices within a large system or network.

## 5 Risk Assessments

### 5.1 General

While the concept of a risk assessment has been around for many decades, many businesses are more familiar with applying the concept to general business risk than to information security. However, an information security risk assessment process is also imperative toward the secure operation and longevity of the technological side of a business. Obviously, in Internet of Things technology, where the engineering team is a critical component to the success of the business, the risk assessment process should be the first step the organisation takes to building a security practice.

While every organisation should create a granular perspective of technological risk, there are high level questions that function as starting points for the risk assessment process, such as:

- What assets (digital or physical) need to be protected?
- What groups of people (tangible or intangible) are potential threat actors?
- What is a threat to the organisation?
- What is a vulnerability?
- What would the consequences be if a protected asset were compromised?
- What is the probability of the asset being compromised?
- What would the result be when put in context with different groups of attackers?
- What is the value of the asset to the organisation and its partners?
- What is the value to the attacker of compromising the asset?
- Could compromise of one or more specific assets lead to the compromise of other assets due to inherent trust between assets?
- What is the impact (e.g. on safety, finance, operation, reputation) of the asset being compromised?
- Are there any special usability requirements (e.g., assistance requirements) that restrict the security mechanisms that can be applied to one or more assets?
- What can be done to detect, remediate or mitigate the potential for vulnerability?
- How can new or evolving gaps in security be monitored?
- What risks cannot be resolved and what do they mean to the organisation?
- What budget should be applied toward incident response, monitoring, and risk remediation?
- Is there a means for 3rd parties who identify a security issue with 1 or more of your assets, products or services to report this to you (e.g., do you have a CVD scheme)?

These starting points will help the engineering and information technology teams work more effectively with the organisation. The goal is to ensure that the technical side of the business agrees on the risks, values, and remediation plans with the executive side of the business. Forcing the teams to work together will help create a more realistic perspective of not only the risk to the business, but the value of assets. This will directly affect the budget that should be applied toward resolving outstanding gaps in security.

There are some risks that simply cannot be resolved. Some of these risks will be discussed in these guidelines. The organisation should evaluate those risks and determine whether they are acceptable. This will provide the business with a realistic understanding of their limitations, the technology’s limitations, and their ability to react to certain types of threats. There is nothing more monetarily draining than presuming that all security gaps can be resolved in a cost-effective manner.

This risk process needs to be applied to both the assets that you own or operate as a business and separately to the products and services (e.g., IoT device or IoT services) that you sell to others.

Many deployments will contain legacy IoT devices. It is therefore necessary as part of the risk assessment to identity how to isolate and protect more secure IoT devices aligned to these guidelines from those which, although still mission critical, cannot be easily upgraded.

Placing legacy IoT devices behind IoT security gateways may be one approach to mitigating the security risks.

### 5.2 Goal

The goal of a risk assessment is to create (or update) a set of policies, procedures, and controls that remediate, monitor, and respond to gaps in security found in the technical part of the organisation. The output of the risk assessment should help the business adjust not only its technology, but the way the technology is managed, designed, and deployed. Once the risk assessment output more adequately describes the value of the information and resources used by the organisation, the overall business can be secured through the enhancement of its personnel, processes, and policies.

Remember, the core benefits to using the output of a risk assessment are:

- Reduced business risk
- Informing personnel
- Known threat landscape applying to your business and its products.
- Enhancing processes
- Defining (or updating) policies
- Executing remediation
- Monitoring for new gaps
- Enhancing the product or service

This essentially helps the organisation enforce a base platform for personnel and process security. This platform then should be incorporated into a cycle that constantly assesses and refines the overall roles and responsibilities of the organisation.

### 5.3 Risk Model References

Rather than attempt to define a risk assessment and threat modelling process here, please review the following references examples for an adequate depiction and walk-through of the risk assessment process:

- National Institute of Standards and Technology (NIST)'s Risk Management Framework [5]
- Computer Emergency Response Team (CERT)'s OCTAVE model [6]
- ETSI TS 102 165 Threat Vulnerability Risk Assessment (TVRA) [41]

## 6 Privacy Considerations

### 6.1 General

Many IoT services and products will be designed to create, collect, or share data. Some of this data may not be considered 'personal data' or impact a consumer's privacy, and therefore, not subject to data protection and privacy laws. This data could include information about the physical state of the machines, internal diagnostic data, or metrics regarding the state of the network. However, many IoT devices may collect, process or store data or security credentials that while in themselves are more privacy sensitive, they may pose a secondary private risk, as they may aid an attacker to in directly compromise other devices or build information may allow an attacker to more accurately target a user (e.g. via user specific customised malware).

However, many IoT services will involve data about or related to individual consumers and will be subject to general data protection and privacy laws. Where mobile operators provide IoT services they will also be subject to telecommunications-specific privacy and security rules. ‘Consumer’ focused IoT services are likely to involve the generation, distribution and use of detailed data that could impact an individuals’ privacy. For example, drawing inferences about their health or developing profiles based on their shopping habits and locations. As consumer IoT services gain in popularity, more consumer data is created, analysed in real-time and shared between multiple parties across national borders.

In current data protection law (e.g., those in the EU), the user must request to explicitly opt in (and give permission for) the processing of data rather than opt out of data processing which was common in older data protection law. The data generated, processed or stored must be the minimum applicable for the purpose for which the user gave consent and that data cannot in general be used for any other purpose for which the user has not explicitly consented (except as specified in law, e.g. for assistance to law enforcement).

The user must have the right to withdraw consent at any time, except for example if bound to a minimum term service contract (e.g. 2-year mobile phone contract).

Most laws define ‘personal data’ as any information that relates to an ‘identified’ or ‘identifiable’ living, natural person.

Where data relates to specific individuals (either directly or by inference), this complex, ‘connected’ ecosystem may raise privacy concerns from the consumer over:

- Has the user consented to their data being collected, processed and stored?
- Who is collecting or processing or storing individuals’ data?
- Is data being sharing between one or more parties?
- What specific data is being acquired?
- Where is the data being acquired from (what technologies or interfaces)?
- When is the data being collected?
- Why is the data being collected from the user, i.e., for which objective is it used?
- How the privacy (not just the security) of individuals’ information is ensured?
- Are individuals in control over how their data is shared and how companies will use it?
- Have you provided a legally compliant means for a user to easily request all data you hold for them (e.g., under EU GDPR).

All providers of IoT services that rely on consumer data – as well as any partner companies capturing or using such data – have an obligation to respect individuals’ privacy and keep personally identifiable or privacy-invasive information secure.

A key challenge for IoT service providers is that there are multiple, and often-inconsistent, laws dealing with privacy and data protection. Different laws may apply in different countries, depending on the types of data involved, as well as the industry sector and services that the service provider is offering. This has implications for a number of consumer oriented IoT service providers.

A connected vehicle, for example, can move between different countries, meaning the associated data transfers may be governed by several different legal jurisdictions. In-car sensors tracking the location of the car (static or dynamic) and its frequent destinations could be used to infer a number of insights about the driver's lifestyle, hobbies or religion, which the driver may consider personal information. Additionally, insights about driving habits through 'on-board diagnostics' sensors might be shared with insurance companies who may use those insights to impose a higher premium and therefore discriminate against the driver without their knowledge.

IoT services and devices (including connected cars) can also move between different sovereign territories and therefore different legal jurisdictions. In many cases, an individual's personal data may transit or reside in jurisdictions different from the individual. These are important issues that need to be considered before a multi-national IoT service is deployed.

Another challenge is that most data protection laws place additional data protection and privacy requirements when handling personal sensitive information– such as health related data.

As more and more devices are connected to the Internet, more and more data about individuals is being collected and analysed. The combination of massive data volumes, cloud storage and predictive analytics can provide detailed profiles of users. In particular, it may become challenging to truly anonymise information and personal information can be inferred from other data types. Similarly, as the number of IoT devices and volume of data they generate increases, both are becoming of ever-increasing interest to attackers.

The need to maintain the privacy of sensitive, health data records is well recognised, not least due to the potential for commercial abuse of such records. In the United States of America, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) includes privacy and security requirements to mitigate the risks of unauthorised disclosure of health records.

HIPAA, like many other regulations such as those in the European Union, only applies if the health data is personally identifiable. The data stored in a blood monitoring device (which does not identify the user) would not be covered by these requirements, whereas that same data in a smartphone app or in a cloud server is likely to be covered because it is able to be linked to an individual (in the case of a smartphone because the phone will almost certainly contain other data identifying the user and in a cloud server because it will be associated with an identifiable user account). Policymakers around the world are realising that information and insights about people can impact their privacy even if they are not defined as 'personally identifiable'. They are therefore beginning to adopt more risk-based approaches to regulation but also considering the wider privacy implications of data use rather than focusing on legal definitions.

To build trust in the IoT ecosystem, governments should ensure data protection and privacy legislation is technology-neutral and that rules are applied consistently to all players in the internet ecosystem. Furthermore, for IoT Service Providers to minimise the need for formal regulatory intervention, we recommend that they follow the recommendations and steps described in Annex A at the early development stages of their IoT devices, services and products.

# 7 Network Security Principles

## 7.1 General

Proper and reliable security mechanisms must be implemented by Network Operators in their networks.

In this section it is described how networks can provide value within the IoT ecosystem. In addition to IoT specific recommendations in this document, it is recommended that operator evaluate their network, management systems and supply chains in accordance with GSMA Baseline Security Controls FS.31 [40].

## 7.2 Secure Identification of Users, Applications, IoT Endpoint Devices, Networks and Service Platforms

Within a cellular connected IoT Service, IoT endpoint devices are identified using IMSI/SUPI and/or IMEI/PEI (EIDs may also be used for devices with eUICCs). Networks are identified using network codes and country codes. Each method of providing identity has varying levels of secure assurance associated with it.

Identity plays a crucial role in the process of authentication as secure authentication can only be achieved on the basis of a secure identity. It is therefore essential that the identities (for example an IMSI, IMEI or ICCID) issued and used within an IoT Service are securely protected against unauthorised modification, impersonation or theft.

One practical problem an IoT Service Provider may face is that their IoT Service may require communications with many IoT Service Platforms, each of which may require a separate unique identification. Each identity used to establish a communications link to each IoT Service Platform will then need to be securely provisioned, stored and managed by the IoT Service.

Where appropriate for the IoT Service, Network Operators recommend the use of UICC based mechanisms to securely identify IoT endpoint devices. Network Operators can also extend the secure storage functionality provided by the UICC (e.g. using IoT SAFE which is described in GSMA IoT.04 [36]) to the IoT Service Provider to enable them to store additional IoT Service-related identities on the UICC.

“Single sign-on” services could also be provided by Network Operators to allow IoT devices to establish and prove their identity once, and then connect to several IoT Service Platforms without further inconvenience. The security trade-offs and risks of using such a service must be considered across the multiple platforms.

## 7.3 IoT Endpoint device and Network Function Assurance

Many parts of a Network Operator’s network will be tested and certified according to international test standards. For consumer IoT endpoint devices it is recommended that they are certified based on ETSI EN 303 645 [25]. Core network function assurance can be achieved through use of GSMA NESAS [35], while assurance of UICCs can be assured through GSMA SAS certification [34].

### 7.4 Threat Management and Information Sharing

The GSMA's Fraud and Security Group (FASG) provides an open, receptive and trusted environment for all Network Operators to share fraud and security intelligence and incident details in a timely and responsible way. The group assesses the global fraud and security threat landscape, analyses the associated risks for Network Operators and their customers and defines and prioritizes appropriate mitigating actions.

### 7.5 IoT Endpoint Device Performance Monitoring and Management

Network operators can measure the performance of the IoT endpoint devices that connect to their networks to isolate IoT endpoint devices that may be creating excessive amounts of radio interference (e.g. do not conform to national regulations) or network signalling traffic (e.g. do not conform with GSMA Connection Efficiency Guidelines [33]) which, in turn, may be degrading the performance of the overall network. IoT endpoint devices can thus be monitored or disconnected when abnormal behaviour is detected.

## 8 Services Provided by Network Operators

### 8.1 General

Network Operators can provide IoT Service Providers with secure cellular and fixed wide area networks (WANs).

This section contains best-practice recommendations when connecting IoT Services to wide area networks. Where appropriate, the recommendations will be independent of the technology used, but will also use best practice from cellular and other network types.

### 8.2 Secure Subscription Management Procedures

This section contains recommendations on how IoT Service Provider subscriptions should be managed by Network Operators:

- The Network Operator or IoT Service Provider should perform an assessment of the network services that are needed to enable the IoT Service (voice, data, SMS, etc.) both now and in the future.
- Based upon this assessment the Network Operator should operate on the "principle of least privilege" and provision the IoT Service Provider's subscriptions with only those services required for the specific IoT Service. For example:
  - IoT Services that only use data bearers should not be provisioned with voice and SMS services.
  - Where an IoT device only connects to a known IoT Service Platform, the subscription associated with the device should only allow connection to a known whitelist of IP address ranges (or domains).
  - If the IoT Service uses voice or SMS, the use of a preconfigured fixed dialling list should be considered.
- Network Operators should identify the UICCs used for IoT Services from traditional UICCs used to provide traditional services and, if required by the IoT Service Provider, segregate these appropriately.

  - If the UICCs used for IoT Services are segregated from the UICCs used for traditional “handsets” then this provides a basis for more secure and efficient management of the associated subscriptions by the Network Operator than might otherwise be the case. For example, a Network Operator might consider using a separate UDM/HSS with security and management optimised to support IoT use cases.

### 8.2.1 UICC Supply and Management

#### 8.2.1.1 Remote management of the UICC (Over-The-Air, OTA)

IoT devices are not physically accessible in some scenarios. To be able to perform changes to the UICCs in IoT devices remotely, UICC OTA management should be supported by the Network Operator as specified by 3GPP.

IoT devices equipped with UICCs need to support the necessary APDU commands to allow remote management of the UICCs.

#### 8.2.1.2 Non-Removable UICC

For improved security, IoT devices should utilise non removable UICCs rather than legacy removal UICCs, where the service threat model suggests that the IoT device may be vulnerable to physical tampering in one or more deployment scenarios. Use of non-removable UICCs is considered desirable in all deployment scenarios from a security perspective.

#### 8.2.1.3 UICC-based Services

A Network Operator might provide an IoT Service Provider with UICC based services such as IoT SAFE which is described in GSMA IoT.04 [36]. This makes it possible for the IoT Service Provider to use the UICC as a secure and tamper resistant platform for their IoT Services. Such UICC-based services are usually developed in JavaCard$^{TM}$ and are interoperable between all JavaCard$^{TM}$ compliant UICC cards. The tamper resistance feature provided by the UICC platform is highly valuable for IoT endpoint devices that can be physically accessed by attackers. Leveraging the UICC as a common secure element for all stakeholders may also make secure IoT endpoint devices more cost effective. See GSMA IoT.04 [36] for further information.

#### 8.2.1.4 Secure UICC Manufacturing and Provisioning

A Network Operators should source their removal UICCs from manufacturers whose manufacturing and provisioning processes are accredited according to the GSMA’s Security Accreditation Scheme (SAS) [34]. For IoT devices provided by an operator (either separately or as part of an Operator IoT Service), the Operator should ensure that the device manufacture has used eUICCs assured according to GSMA SAS [34] within the IoT device.

## 8.3 Support of Non-IP Communications Protocols

Network Operators provide several types of communication services that can be used by an IoT Service, such as USSD, SMS, RCS [37] and IP data connectivity. While IP connectivity (Mobile 3GPP or WIFI) is most commonly used by IoT devices, SMS, RCS and USSD may be used for specific messaging application requirements.

USSD and SMS have limited security support capabilities. In general, USSD and SMS traffic is not by default ‘end to end’ cryptographically protected by the Network Operator and cryptographic protection mechanisms to ensure confidentiality and integrity are not available for SMS messages. IoT Service Providers that use USSD or SMS for their communication need to be aware of the vulnerabilities associated with USSD and SMS and, where possible, implement additional encryption at the service layer.

GSMA RCS which is increasingly supported within all Smartphones from 2023 onwards should be considered by operators and manufacturers as a more secure alternative to SMS or USSD in IoT Devices, Products and Services.

## 8.4 Security of Low Power Wide Area Networks

Several Low Power Wide Area (LPWA) network technologies have been deployed by various network operators. A full and up-to-date list of LPWA network deployments can be found on the GSMA website: www.gsma.com/iot

GSMA Deployment guide for Mobile IoT [38] can help ensure the consistent deployment of these technologies from both a network and device perspective.

Given that most LPWA technologies over lower security strength than 3GPP based RANs or strong WIFI security, use of LPWA should be subject to a security risk assessment.

As a minimum, the following important network security factors should be considered:

- Bandwidth, including Maximum Downlink and Uplink Data Rates – This may limit the security features that can be supported by the LPWA network or implemented in the application layer.
- Daily Downlink and Uplink Throughput – LPWA devices do not typically transmit or receive data all of the time which can impact security features such as over-the-air security updates.
- Authentication – Device, Subscriber and Network – Secure network connectivity requires a number of different parties to authenticate themselves to each other such as the device, the subscriber and the network provider – the technology must protect against the ‘spoofing’ of these parties by malicious actors.
- Data Confidentiality – Encryption is typically used to keep data safe from being intercepted by an attacker. Trust in this can be increased by establishing end-to-end security at the application layer.
- Key Provisioning – Cryptographic techniques for authentication, confidentiality and integrity all rely on cryptographic keys being securely shared between parties.
- Certified Equipment – In many markets there are legal requirements for devices with radio transmission to have approval or certification before being sold. This is an opportunity for security features to be verified.
- IP Network – Use of IP can open up the possibility of attack on devices from the internet and IP security features must be considered.

It is noted that important security features of LPWA technologies may be optional in some technologies and therefore network operators should ensure that these features are supported and enabled by default in their deployments. Similarly, IoT device manufacturers should ensure that IoT devices support these features and that they are enabled by default.

The network operators must ensure they are aware of the security consequences of the choices they make in their network configuration and to ensure that the state of these options is clearly communicated to their customers.

Specific security consideration when using a LPWA technology include:

For All LPWA Network Technologies:

- Whether an IP network layer is implemented over the link layer.
- Whether a secure element is present, and if so, whether it is removable.
- To what extent data integrity is guaranteed.
- Whether any algorithms or key lengths supported by the technology are no longer recommended by government security catalogues (e.g. FIPS) or should be deprecated (such as 64-bit encryption keys for GPRS).

For 3GPP LPWA Network Technologies (i.e. NB-IoT and LTE-M):

- Whether Remote SIM Provisioning (RSP) is supported.
- Which integrity algorithms (EIAx/GIAx) and confidentiality algorithms (EEAx/GEAx) are implemented and permitted.

For LoRaWAN:

- Whether ABP (Activation By Personalisation) or OTAA (Over-The-Air Activation) is implemented, and for OTAA whether an AppKey may be shared between devices.

For SigFox:

- When using SigFox network, it must be taken into account that payload encryption is optional but available. Therefore, a Sigfox certified crypto chip must be used to enable the AES 128 encryption and keep data confidential over the air.

For All LPWA Devices:

- What form (if any) of security certification has been undertaken.

### 8.4.1 IoT Device Signal Storms and Network Attacks Mitigation

IoT devices and services may have additional security requirements from the mobile network, compared to general smartphones. While serving a large number of IoT devices, the mobile network may be exposed to signalling storms. An intentionally malicious Denial of Service attack is only one reason for such storms.

Extended Access Barring (EAB) service as defined in 3GPP TS 23.122 [29] may be useful in mitigating such scenarios. Network Operators can restrict network access to the IoT devices configured for EAB, in addition to common and domain-specific access control mechanisms. EAB configuration can be performed in the UICC or in the IoT device itself.

There may also be a need for the Network Operator (together with the IoT Service Provider if different) to distinguish between low priority IoT devices, and critical IoT devices. For example, it may be necessary for healthcare devices to continue to maintain service under signalling storms and service denial attacks. There may be a need for Network to reject the registration of ‘low priority’ IoT devices under signalling storm conditions, but to allow ‘high priority’ IoT devices to register and maintain service.

Roaming IoT devices present additional risks to serving networks in roaming scenarios. The general recommendation would be for Network Operators to screen all roaming messages received from home networks/roaming partners in relation to IoT devices, or services. In addition to blocking messages from unauthorized/faked home networks/roaming partners, there is a need may be a need to filter the messages according to the IoT device priority.

Similarly, home networks may be exposed to signalling or data volume attacks caused by large numbers of roaming IoT devices distributed across one or more visited serving networks, especially where serving network security is weaker than that of the home network (e.g. from visited network in countries where encryption may be switched of or of limited strength).

### 8.4.2 IoT Endpoint Device Block Listing

Network Operators should implement IoT device block / barring list and connection to the GSMA Central Equipment Identity Register (CEIR) database. The CEIR is a central database, administered by the GSMA, containing IMEIs associated with lost and stolen devices (including Smartphones and Cellular IoT devices) that should not be granted network access. Once an IMEI is entered into the CEIR the IoT device containing the IMEI will be block listed by all Network Operators who take that data and implement local block listing based on their use of equipment identity registers (EIRs).

Network Operators may also implement localised device block listing to allow the temporary suspension of ‘suspect’ devices whilst the Network Operator investigates the nature of such devices prior to any CEIR block listing. It should be noted that for critical services such as healthcare, blocking an IMEI may not be desirable. It is important that the details of connected safety critical IoT devices should be clearly understood by Network Operators in so far that the true application (or host) of an IoT device can be discerned. IoT devices that leverage the IMEI issued to a communications module vendor should support Device Host Identify Reporting which is a capability that enables the IoT device to report host information to the Network Operator.  Device Host Identify Reporting is described in the GSMA’s Connection Efficiency Guidelines [33].

### 8.4.3 Analytics-based Security

Network Operators can provide data analytics and traffic filtering services to identify threats in IoT Services.

This may be especially useful for restricted IoT devices (e.g. limited compute or battery power devices) where the devices or associated services cannot provide this functionality themselves. Network Operators can provide IoT Service Providers and customers with visibility of the security status, identified threats and attacks to their IoT devices.

# 9 Using This Guide Effectively

## 9.1 General

While security is best implemented at the start of an engineering project, this guide can also assist in organisations that have already designed, fabricated, and even deployed an IoT product or service. Regardless of which stage the reader's product or service has reached, there is a useful process that should be followed to get the most benefit from this set of documents:

- Evaluate the technical model;
- Review the current product or service's Security Model;
- Review and evaluate Recommendations;
- Implementation and Review;
- Ongoing Lifecycle

## 9.2 Evaluating the Technical Model

The first and most important step in the process is understanding the organisation's own IoT product or service. To perform a security review and risk assessment, the team should be familiarised with each component used in the organisation's solution, how components interact, and how the components interact with their environment. Without a clear understanding of how the product or service was (or will be) built, a review will be incomplete.

Start by making a document describing each component used in the system. Identify how the component is sourced, how it is used, what privilege level it requires, and how it is integrated into the overall solution. Map each component to the technologies described in the Model section of this Ecosystem [4] and Service Ecosystem [3] guidelines documents. It is acceptable if the document doesn't specifically match a component, as it should map the component's general class. Simply use the class of component, such as a microcontroller, communications module, or trust anchor, as the context. Consider the following questions:

- What components are used to build the product or service?
- What inputs and outputs are applicable to the given component?
- What security controls are already applied to these inputs and outputs?
- Has the least privilege level necessary been applied to each component?
- Who in the organisation is responsible for implementing or sourcing the component?
- Who in the organisation is responsible for monitoring and managing the component?
- What process is in place to remediate risks observed in the component?

These questions, when answered, will provide an understanding of how the technical components interact with each other, and how the overall product or service is affected by each component.

This process corresponds with the first and second phases of the CERT OCTAVE risk assessment model [6], or the Frame stage of the NIST Risk Management Framework [5]. This assists in the development of a profile for each critical business asset, the development of security objectives, and establishes a foundation for how the company will assess, monitor, and respond to risk.

## 9.3 Review the Current Security Model

Next, read through the security model section of the Endpoint IoT device or Service being assessed. This section will help the reader understand the model that an attacker will use to compromise a given technology. This model is based on years of experience performing security assessments on, reverse engineering, and designing embedded systems.

Once the security model has been reviewed, the reader should have a better understanding of what technologies are most vulnerable, or most desirable to the attacker, in the product or service being developed. This information should be shared with the organisation, to ensure that both engineers and leadership understand the risks and threats to the current model.

However, it should be noted that the organisation should not take steps to adjust their security model at this time. It is too early to make concise architectural changes.

This process again corresponds to the first and second phases of the CERT OCTAVE model [6], or the Frame stage of the NIST Risk Management Framework [5]. Reviewing the security model helps enhance the technical model by identifying potential gaps in security and shining a spotlight on security objectives that should be prioritised.

## 9.4 Review and Evaluate Recommendations

The Recommendations section should be reviewed at this time to evaluate how Security Tasks can be resolved. This section will not only provide methodologies for implementing recommendations but will provide insight into the challenges involved in implementing specific recommendations.

For each recommendation, a Method section is provided. This section will outline methodologies that assist in the remediation or mitigation of the corresponding security risk. These methods, while presented from a high level, outline concepts that reduce risk from a holistic perspective, to ensure the greatest amount of gain is acquired from a reasonable and practical amount of effort.

An Expense section is provided to discuss, where applicable, extra financial expenses that the organisation should prepare for when implementing a particular recommendation. While most expenses, such as engineering time and raw materials, are fairly obvious, less obvious expenses can alter the finances applied to products and services whose profit margins and budgetary limits have already been defined by the business leadership. While specific numbers are not provided, technologies and services are specified that may incur additional costs.

A Risk section is also provided so the reader understands the gaps in security that are likely to result from not implementing a particular recommendation. While the business may accept that some risks are within the business's operating guidelines, the reader should review each risk section to ensure that the business fully understands the side effects of not implementing (or not correctly implementing) a given recommendation. This may seem straight forward for recommendations such as “Encrypt Data”, but the subtlety of some threats, such as replay attacks against messages that are not cryptographically unique, may be a surprise to the reader at a later date.

In some cases, references are provided for further review. While this document does not provide detailed information on every technology, risk, or remediation plan, other standards and time-proven strategies do. This set of documents provides references to those materials, where applicable, within each recommendation.

The output from reviewing the Recommendations section should directly tie into the Security Tasks section. The Security Tasks should now be filled out with Recommendations that are appropriate for implementing the Security Tasks correctly. These Security Tasks will then tie back to specific components assigned to members of the organisation.

Evaluating recommendations corresponds to the Assess step of the NIST Risk Management Framework [5], and steps six, seven, and eight of the CERT OCTAVE methodology [6].

## 9.5 Implementation and Review

By this stage, clear Security Tasks have been outlined and the business will have a better comprehension of their security vulnerabilities, their value and their risk. The business shall now create a clear architectural model for each component being adjusted and use the risk assessment process chosen by the organisation to develop a threat model for each component, incorporating the recommendations and risks that are appropriate for each component and Security Task. When the architectural model is completed, the organisation can begin implementing each recommendation in order to fulfil the Security Tasks.

When the implementation is complete, the organisation should review the risks in both the Recommendations subsection and the Component sections. The organisation should ensure that the implementation fulfils the requirements set forth by these sections. The organisation should then ensure that the implementation solves security with regard to the context in which the component is designed in the organisation’s product or service, as these documents cannot fully address every product or service being designed in the field. If possible, have a third-party consulting firm evaluate the implementation to ensure that it does indeed adhere to security best practices.

Implementation and review correspond with the Respond component of the NIST Risk Management Framework [5], and step eight of the CERT OCTAVE model [6].

## 9.6 Ongoing Lifecycle

The security life cycle does not stop at this juncture. Rather, security is an inherent part of the overall engineering of a process. IoT devices and IoT services have a lifetime and must be continually serviced throughout that lifetime. This needs to be considered both in terms of the lifecycle of the product and the data lifecycle generated, processed or stored by those products.

Requirements change over time. Cryptographic algorithms become dated or deprecated. New protocols and radio technologies must interoperate with the product or service. This ever-changing ecosystem in which our embedded products are deployed, must be constantly reviewed to ensure that confidentiality, integrity, availability, and authenticity are maintained.

Managing the ongoing security lifecycle corresponds with the Monitor and Frame components of the NIST Risk Management Framework [5], and steps one, four, and five of the CERT OCTAVE model [6].

For IoT devices it is necessary to consider how the ownership of a device may change during the lifetime of the device and what happens at the end of the device's usable lifespan. Can data be securely erased and the device reset back to a factory state by the owner if required? Similarly with EU repairability (or equivalent) requirements, has security and privacy impacts been considered if security or privacy critical components need to be replaced during the lifespan of the device.

# 10 Example – Wearable Heart Rate Monitor

## 10.1 General

In this example, a simple Heart Rate Monitor (HRM) design will be evaluated using this set of guidelines. The IoT device will be assessed using the IoT device Ecosystem document, while the service side of the design will be assessed using the Service Ecosystem document.

## 10.2 The IoT Device Overview

First, let's start by evaluating the hardware design of the IoT device.

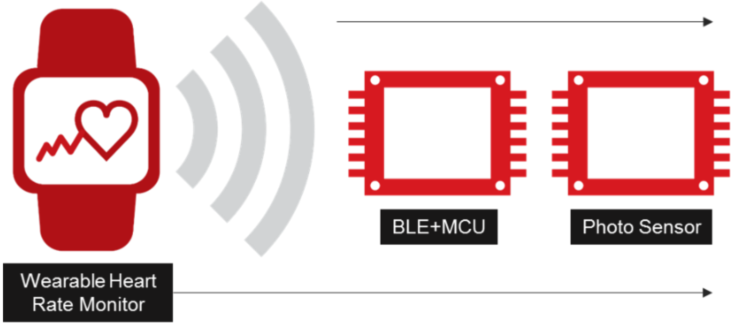

**Figure 4 – Simple HRM and Primary Components**

The HRM is composed of standard components for a simple wireless wearable device: an ambient light photo sensor and a Bluetooth Low Energy (BLE) transceiver enabled microcontroller. The sensor is used to capture pulse rate data, while the microcontroller analyses the data emitting from the sensor and chooses what data to send over the built-in BLE transceiver. In this example, the BLE stack used is version 4.2.

A coin cell battery is used in this example to transmit data from the HRM to another device, such as a smart-phone or tablet. No other components are required for this device to function.

According to the IoT Endpoint Ecosystem document [4], this device would fit into the Lightweight Endpoint class of devices.

## 10.3 The Service Overview

From a service perspective, the application on the smartphone or tablet pushes metrics from the IoT endpoint device up to a back-end service over any available network connection. The back-end service for the application simply associates the device owner with the metrics being captured and stores them in a database local to the application server.

Visualisation of the data can be achieved using the mobile application, or via the service's website. Users of the wearable technology can log into the service provider's website to perform more actions with the metrics captured by the IoT device.

This is a very simple and common service model with no custom or unnecessary complexities.

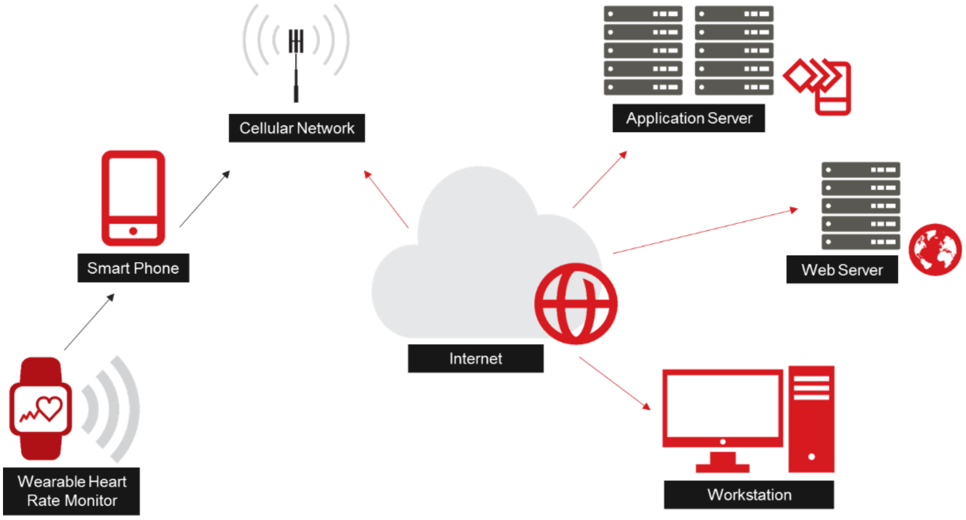

**Figure 5 – Flow of Data to Simple Back End Service**

## 10.4 The Use Case

The business developing this technology intends the end user to track their pulse data throughout the day, storing it in both the application and the back-end database. The intention is to allow users to review their heart rate over time to track their overall health. Users can watch their health improve or worsen over time, depending on whether they are maintaining a healthy lifestyle. This allows the users to incentivise themselves by evaluating both positive and negative trends in their HRM data.

The business intends to use this data to partner with medical device manufacturers, health care providers, and other organisations that can use these metrics to identify whether a consumer is more or less likely to incur a health-related event, such as a heart attack or a stroke.

## 10.5 The Security Model

The engineering team at this example business leveraged the frequently asked security question sections of the IoT Endpoint [3] and Service [4] documents, to determine what issues are most relevant to their product and service.

From an IoT endpoint perspective, the team learned the following issues are of concern:

- Cloning
- IoT device impersonation
- IoT Service impersonation
- Ensuring privacy

From a service perspective, the team decided the following issues are of concern:

- Cloning
- Hacked services
- Identifying anomalous IoT device behaviour
- Limiting compromise
- Reducing data loss
- Reducing exploitation
- Managing user privacy
- Improving availability

The team reviewed the recommendations for each of the above issues, as suggested by each relevant frequently asked security question section. The team then chose to implement recommendations that were cost-effective improvements ensuring the greatest amount of security.

In this example model, the IoT device would not require a substantial change. Since the IoT device has very little functionality, minimal security can be employed on the IoT device for both application security and communication. Since the IoT device application is flashed on a single device, as long as the device firmware is locked, there is no significant threat of attack against the IoT device within the given use case.

However, since privacy is an issue, the organisation should employ at least a personalised PSK version of a Trusted Computing Base (TCB). This would ensure that encryption tokens were unique to each IoT device, so that one compromised IoT device cannot compromise all IoT devices. If the personalised (unique) keys were encoded into the locked microcontroller, it would be reasonable to believe that this use case were adequately secured from the threat of cloning, impersonation, and privacy issues. Review the IoT Service [3] and IoT Endpoint [4] documents for a more complete discussion on what a Trusted Computing Base is within each ecosystem’s context.

The server infrastructure, however, requires a significant number of changes. The engineers realise that, according to the recommendations, they are at serious risk of abuse. The following issues are acknowledged:

- There is no security front-end diminishing the effects of a Denial of Service attack.
- There are no ingress or egress controls limiting the flow of traffic to or from services.
- There is no separation of duties between service tiers.
- There is no separate secured database containing personalised PSK tokens.
- No adequate security measures are implemented in the service operating system.
- There are no metrics taken to evaluate anomalous IoT device behaviour.

## 10.6 The Result

After implementing the recommendations, the organisation has a much better-defined back-end service architecture that adequately addresses the risks identified through the guidelines.

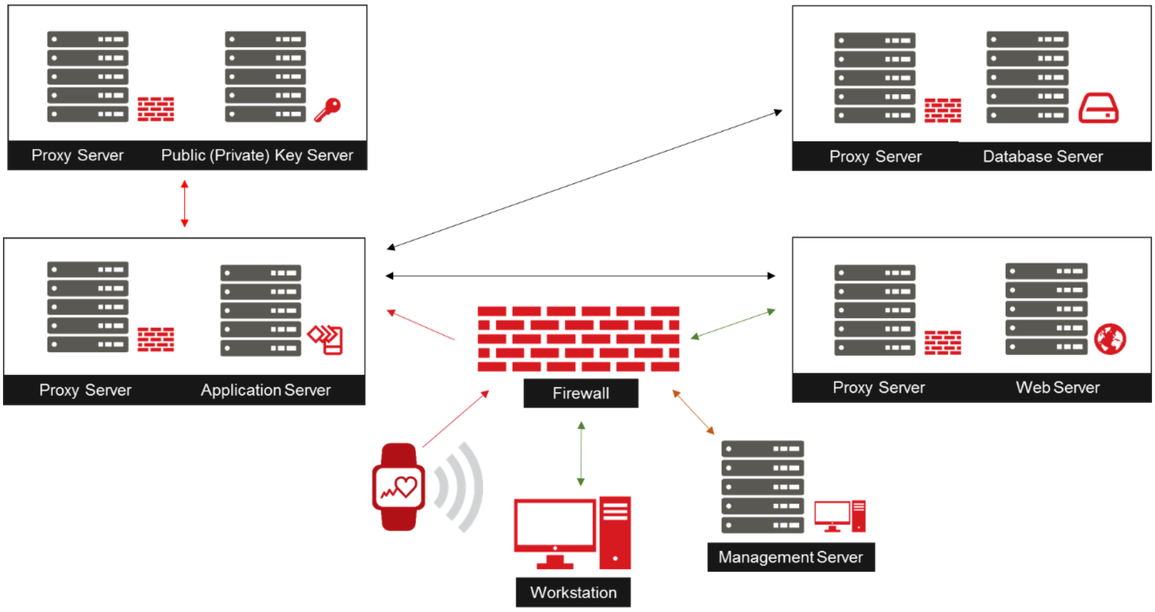

**Figure 6 – Resultant Service Ecosystem**

In the above figure, the changes to the service ecosystem are easily observable. Each class of service has been broken into separate tiers to help secure and scale the technology easily if demand spikes. Two additional tiers were added, a database tier and an authentication tier, to separate critical systems from services that directly interface with the outside world. A security front-end was implemented to help guard the internal network from multiple types of attacks, including DoS and DDoS attacks that reduce the overall availability of the system. Finally, an administrative model was defined to allow management secure access to the production environment. One component not depicted in the above diagram is the presence of an analytics model that observes when IoT device behaviour may be indicative of a compromise, or a flaw in the firmware or hardware design.

## 10.7 Summary

Overall, this simple technology could have been easily compromised had it been deployed “as is”. Yet, with a few fast, simple, and cost-effective changes made on the IoT device, the technology is assured to have years of longevity in the field without change to the architecture.

With the service ecosystem ramped up, there is far less of a threat to both users and the business. Cloning and impersonation is no longer a threat. Privacy is ensured by granting each IoT device unique cryptographic tokens. Systems that contain critical information are separated and secured from more heavily abused public-facing systems. This model, while slightly more complex, reduces the overall risk of the production environment.

# 11 Example – Personal Drone

## 11.1 General

In this example, a small personal drone device will be evaluated using this set of guidelines. The IoT device will be assessed using the Endpoint Ecosystem document [4], while the service side of the design will be assessed using the Service Ecosystem document [3].

## 11.2 The Endpoint Overview

First, let's start by evaluating the hardware design of the IoT device.

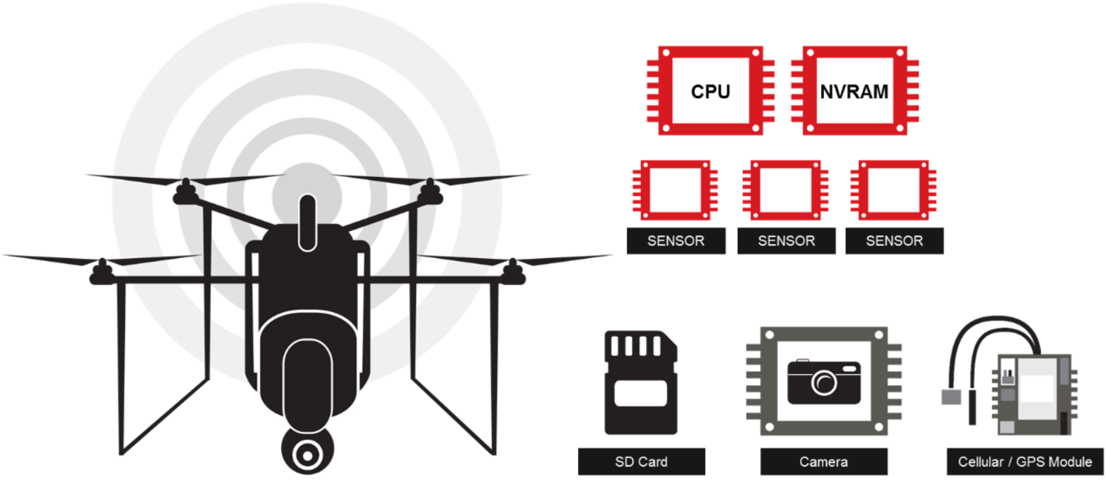

**Figure 7 – A Drone and its Primary Components**

This personal drone is composed of a robust set of components. The processing capabilities of the drone are high performance due to the multiple motors, sensors, and other equipment that all must function efficiently in parallel. This example model uses an ARM Cortex-A8 CPU with the primary operating system (Linux) stored in NVRAM on a separate chip. An array of various sensors is required for detecting movement, light, speed, and location. A SD/MMC card is used to store video, sensor metrics, and metadata. A camera is used to allow the operator to see from the drone's perspective. A cellular/GPS combination module is used to ensure the drone can maintain connectivity to its operator even when it is out of range of a proprietary protocol. GPS is also used for guidance, and for minimal automation.

A Lithium Polymer (LiPo) battery is used to drive the drone. Its flight time is approximately two hours before a new charge is required when all functions are active at once.

According to the Endpoint Ecosystem document [4], this device would fit into the Complex Endpoint class of IoT devices. Even though it contains a cellular module, it is not considered a gateway as it does not route messages to or from other IoT devices.

## 11.3 The Service Overview

From a service perspective, the back end is only used for operator connectivity when loss is detected on the proprietary radio interface during flight. If the drone is in flight and the cellular connection can be enabled, it will attempt to wait for its operator to connect via the cellular network (e.g. 5G). If, however, it is unable to be controlled over the cellular network, it will attempt an automated landing at the location where it last lifted off.

However, as the drone has some light automation features, it can be given coordinates and a path to traverse while taking photos or short videos. These media files can be uploaded in real time over the cellular network to the back-end service to show the operator its course and viewpoint during automated execution.

Thus, a robust back-end service is required to ensure a high degree of service availability for each drone that might connect to the system. Availability is also necessary for the high bursts of network traffic required to transmit videos and high-resolution images over a cellular link. There must also be a web interface that allows the operator to view media uploads from a web browser.

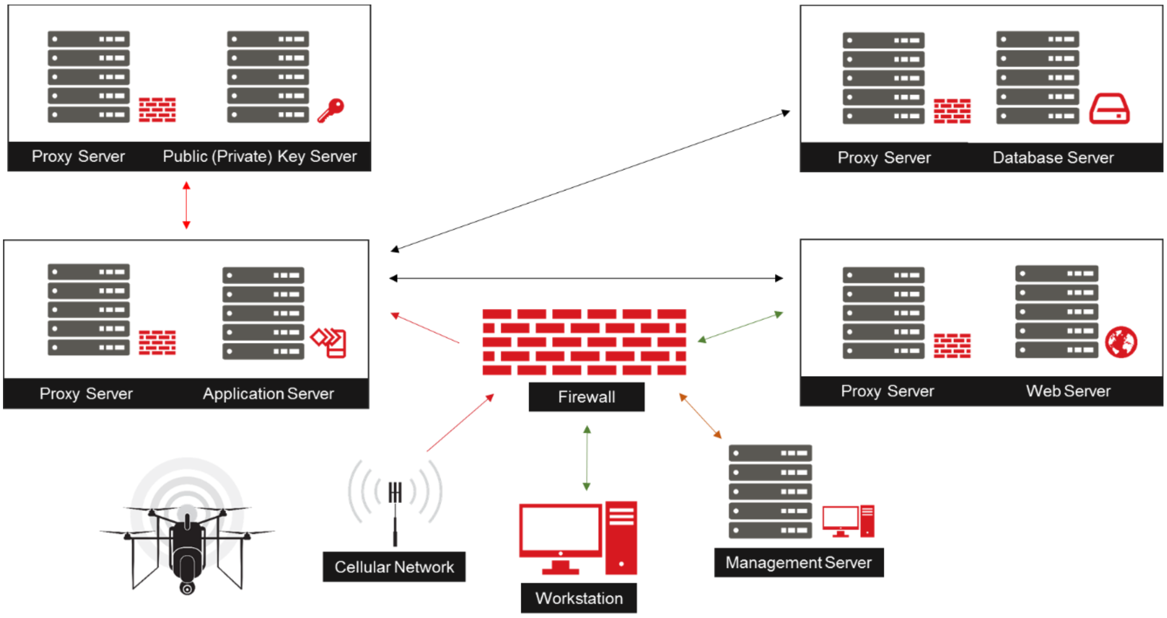

**Figure 8 – Flow of Data to Back End Services**

## 11.4 The Use Case

The business developing this technology intends the end user to use the drone for filming in the wild. However, some of their customers have used the drone for filming scenes in cinema, as the camera and stabilisation capabilities of the drone are exceptional for the price point. As a result, the drone may be used in expensive filming projects where intellectual property and privacy are major concerns.

## 11.5 The Security Model

The engineering team at this example business leveraged the frequently asked security question sections of the Endpoint [4] and Service [3] documents to determine what issues are most relevant to their product and service.

From an IoT endpoint device perspective, the team learned the following issues are of concern:

- IoT device identity
- IoT device impersonation

- Trust anchor attacks
- Software and firmware tampering
- Secure remote management
- Detecting compromised IoT devices
- Service impersonation
- Ensuring privacy

From a service perspective, the team decided the following issues are of concern:

- Managing user privacy
- Improving availability

The team reviewed the recommendations for each of the above issues, as suggested by each relevant frequently asked security question section. The team then chose to implement appropriate security mechanisms to mitigate the identified threats and reduce the risks to an acceptable level.

In this example, the service infrastructure does not require a substantial change. This is because the service infrastructure already had to be built out extensively to accommodate for the bursts of traffic required in servicing the IoT endpoint device. The architecture already demanded a well-formed and secure architecture simply to be able to scale effectively and maintain availability of resources even when some services were incurring temporary faults. However, the organisation chose to investigate user privacy further as this has become a primary point of contention for the business's unexpected niche.

The IoT device infrastructure, however, requires a significant number of changes. The engineers realise that, according to the recommendations, they are at serious risk of abuse. The following issues are acknowledged:

- The bootloader is not properly validating the application prior to executing the operating system kernel, leading to a risk of tampering.
- There is no TCB used to manage the security of the application or communications.
- Because there is no properly implemented TCB or trust anchor, IoT device impersonation is a problem, which may lead to data leakage.
- Without a well implemented TCB, the IoT device can't securely authenticate services.
- Without a well implemented TCB, the IoT device can't securely authenticate the operator over the proprietary radio interface.
- The engineers have relied on the security of the cellular network to ensure the communications channel can't be compromised but have not considered the threat of IoT device impersonation or Femtocell repurposing, both of which bypass the security of the cellular network to compromise weak service security.

## 11.6 The Result

After implementing the recommendations for the issues cited above, the organisation has a much better defined IoT endpoint device architecture that adequately addresses the risks identified through the guideline documents.

For the existing drone system already in production, the engineering team issues a firmware update that implements a unique public key security model. The firmware update improves the bootloader as well by baking security into the core architecture. Since a unique public key model was used, anyone attempting to abuse the initial lack of security in the IoT device to attempt to impersonate another user's IoT device would fail, as the engineers leveraged their existing user-to-IoT device mapping database to create unique keys on a per-user basis. This way, no user without the appropriate web credentials can download and install another user's unique public key update. While this process was complex and time consuming to implement, it will be worth the effort.

Future versions of the drone technology will implement an internal CPU trust anchor. This trust anchor will be tied to a TCB, to ensure that each IoT device is uniquely seeded with risk appropriate security from the ground up.

Deploying strong cryptography in this fashion is imperative, as it also negates the potential for the other classes of attack the company identified as a concern. By leveraging the benefit of strong cryptography and a TCB for verification and authentication, the engineering team can easily identify whether rogue services are being made available to the drone. The drone, upon detecting rogue services, can simply land back at the original take-off site.

Any service that detects an improperly secured drone can also raise flags internally. The administration team, at that time, can determine how to deal with the potentially compromised drone. This provides a level of agility with regard to security events, and also gives the organisation a way to evaluate if there are software or hardware problems that are causing abnormal behaviour on the IoT endpoint device.

### 11.7 Summary

While the engineering team obviously spent a significant amount of time creating a resilient architecture from a mechanical engineering and back-end services perspective, substantial additional work was needed to appropriately secure the IoT endpoint device. While this scenario did not pose a critical threat to the overall business, it was fortunate that there was a solution that worked well enough for their customer's needs. Had this been a more safety-critical technology, even the solution deployed here may have not been sufficient.

For more information on Trusted Computing Base variants, please review the IoT Service [3] and Endpoint [4] Ecosystem documents.

## 12 Example – Vehicle Sensor Network

### 12.1 General

In this example, a vehicle sensor network deployed in a new class of automobile will be evaluated using this set of guidelines. The IoT devices making up the endpoint will be assessed using the Endpoint Ecosystem document [3], while the service side of the design will be assessed using the Service Ecosystem document [4].

### 12.2 The IoT Endpoint Device Overview

First, let's start by evaluating the hardware design of the IoT devices that make up the endpoint.

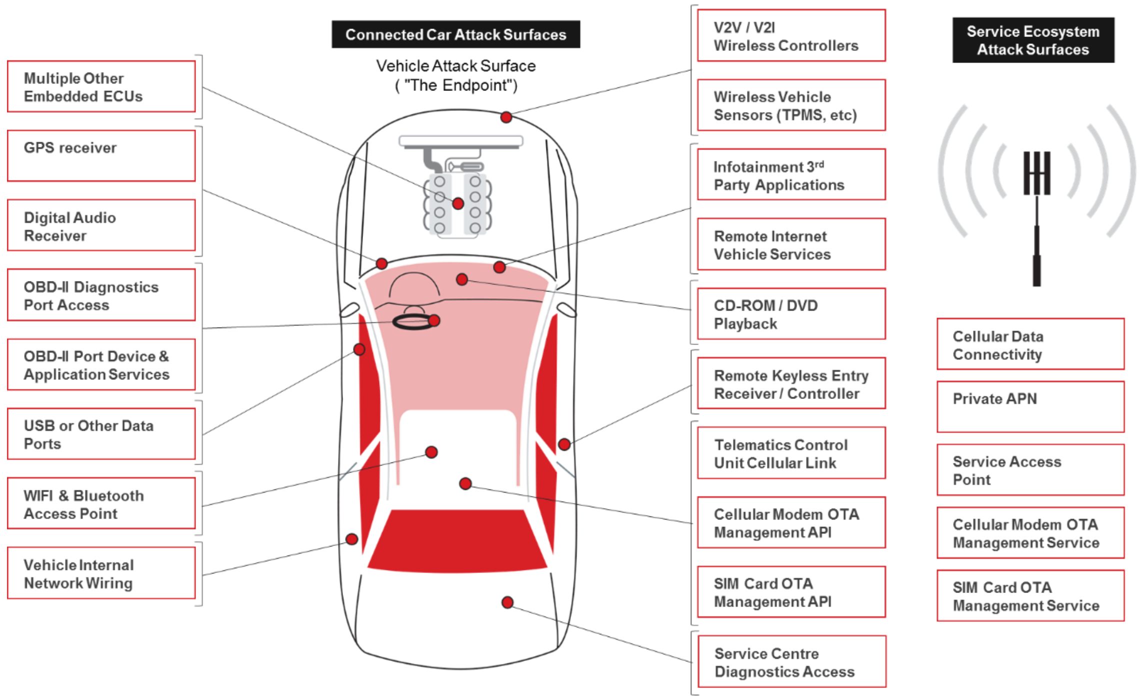
Connected Car Attack Surfaces
Vehicle Attack Surface
( "The Endpoint")
Multiple Other Embedded ECUs
GPS receiver
Digital Audio Receiver
OBD-II Diagnostics Port Access
OBD-II Port Device & Application Services
USB or Other Data Ports
WIFI & Bluetooth Access Point
Vehicle Internal Network Wiring
V2V / V2I Wireless Controllers
Wireless Vehicle Sensors (TPMS, etc)
Infotainment 3rd Party Applications
Remote Internet Vehicle Services
CD-ROM / DVD Playback
Remote Keyless Entry Receiver / Controller
Telematics Control Unit Cellular Link
Cellular Modem OTA Management API
SIM Card OTA Management API
Service Centre Diagnostics Access
Service Ecosystem Attack Surfaces
Cellular Data Connectivity
Private APN
Service Access Point
Cellular Modem OTA Management Service
SIM Card OTA Management Service

**Figure 9 – Connected Car Attack Surfaces**

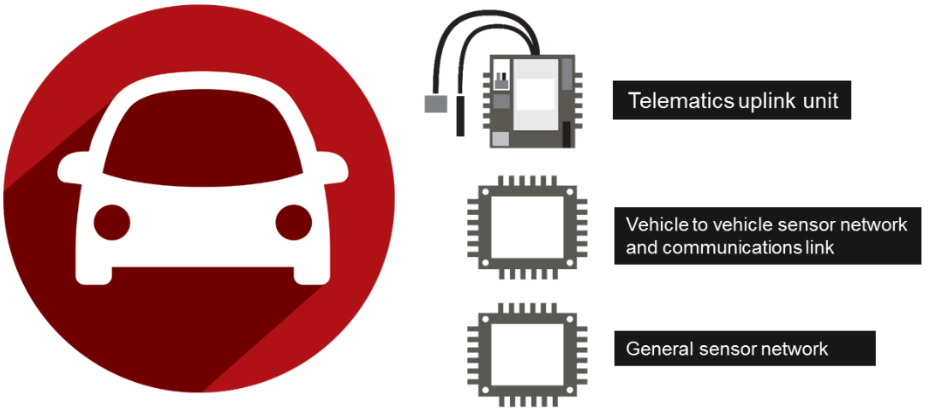

**Figure 10 – Full Vehicle Sensor Network and Communications System**

While the model in Figure 9 is too complex to properly depict in a simple diagram, the three high-level components involved are (as shown in Figure 10):

- A telematics uplink unit that manages the sensor network, makes complex decisions on behalf of the driver, and maintains a connection to the back-end system.
- A vehicle-to-vehicle (V2V) system that detects and reacts to V2V events.
- A general sensor network that provides metrics to the telematics uplink unit.

In modern automotive systems, the telematics unit is a part of the automobile’s computer network and makes decisions based on sensor data and back-end communications. This unit will make decisions with, or on behalf of, the consumer driving the vehicle. The unit ensures that the vehicle is operating properly, attempts to make intelligent decisions during emergencies, and takes commands from the back-end network.

The V2V sensor network identifies vehicles in the vicinity and makes decisions based on metrics gathered from sensors. While the telematics unit primarily makes decisions based on the state of components (such as brakes or tire pressure monitors), the V2V system makes decisions based on the presence of other vehicles or sends out alerts to nearby vehicles in the case of a critical event.

The general sensor network is a series of components that provide data to the telematics unit, and sometimes the V2V unit. These units use the information gathered from the general sensor network to make accurate decisions during critical events.

According to the Endpoint Ecosystem document [4], this system has components that fit into every IoT endpoint class. The telematics uplink unit acts as a gateway. The V2V unit acts as a complex endpoint. The general sensor devices are effectively all lightweight endpoints.

## 12.3 The Service Overview

From a service perspective, the vehicle sensor network will provide metrics to the back-end environment. This data may or may not be provided to the consumer. Rather, the data could be stored by the manufacturer to observe or identify potential problems with components. This may trigger service warnings that are then issued to the consumer.

The system may also be augmented to provide the consumer with useful services, such as “remotely unlock door”, “start engine”, and similar features. In future, these systems may allow vehicles to be driven remotely through automated guidance systems.

While safety critical decisions will be made locally in the processing units on the vehicle itself, some decisions may be supported by information from the cloud sent over the cellular network or shared directly within a local geographic area between vehicles. It is assumed that both the endpoint IoT devices in the vehicle and supporting cloud services will utilise AI for enhanced decision making.

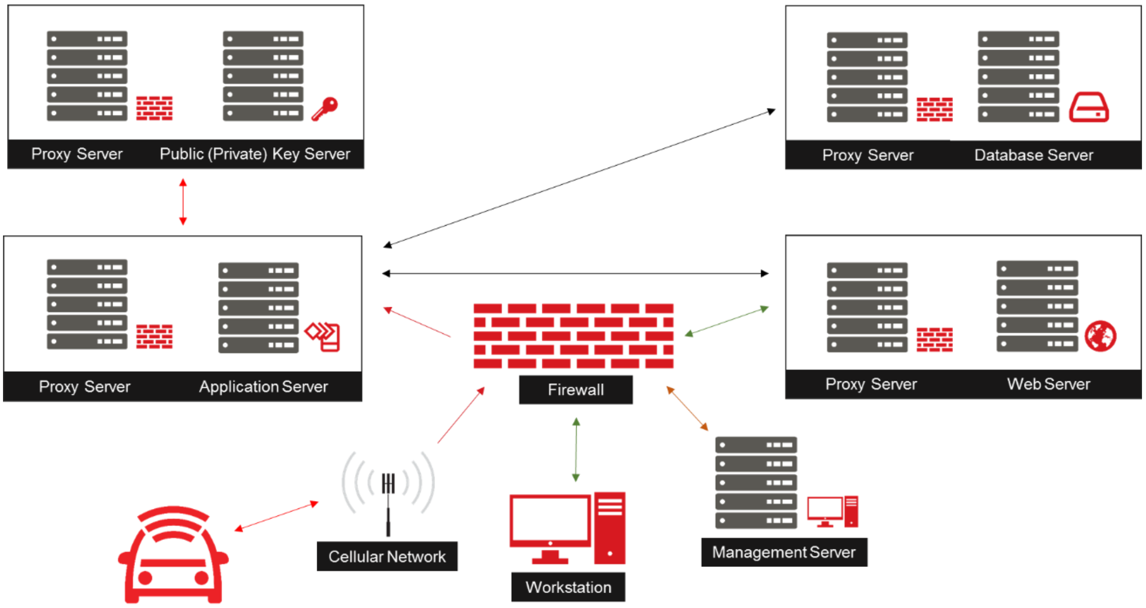

**Figure 11 – Flow of Data to Back End Services**

## 12.4 The Use Case

The use case of this technology is obvious: to build smarter vehicles that can make complex decisions in safety-critical scenarios. The goal is to leverage the intelligence of as many sensors as possible to make critical decisions in very small windows of time. Automatic breaking, tyre blow-out broadcast alerts, temporarily disabled operator warnings, and other critical scenarios can potentially be resolved using sensors and well-designed computer systems.

One interesting feature of this technology is that it may be entirely transparent to the driver (user). The user would not need to configure these endpoint systems to act in a certain fashion. Instead, they should be capable of negotiating the current landscape through the use of sensor metrics.

## 12.5 The Security Model

The engineering team at this example business leveraged the frequently asked security question sections of the Endpoint [4] and Service [3] documents to determine what issues are most relevant to their product and service.

From an IoT endpoint device perspective, the team learned the following issues are of concern:

- IoT device impersonation
- Service or peer impersonation
- Side-channel attacks
- Detecting compromised IoT devices
- Ensuring safety at the risk of security

From a service perspective, the team decided the following issues are of concern:

- Identifying anomalous IoT device behaviour

- Managing user privacy

However, since the endpoint (vehicle) is made up of a large number of IoT devices with different functionality and criticality the team must assess the threats and risks applicable to each individual IoT device. Additionally, the team must assess how groups of endpoint IoT devices work together to provide specific functions (e.g., steering control) and consider additional isolation or prioritisation requirements that apply to those groups.

Each IoT device may support multiple functionalities within the endpoint eco-system (e.g. reversing camera and control of infotainment system) and therefore isolation of these functionalities must also be considered within the design each IoT device within the overall endpoint eco-system.

The biggest risk to this environment that hasn't been discussed in previous examples is the risk of impersonation with regard to peers. One concern that engineers have in this type of environment, is the risk that a IoT device or group of devices will make critical decisions using data that is not properly authenticated.

Since sensor data in critical scenarios requires fast processing times, it is often incorrectly assumed that it may not always be feasible to implement any or adequate, security protection mechanisms, if they introduce overhead or delay. Approaches such pre-establishment of communications paths or pre-sharing of unique security credentials ahead of time can allow appropriate security mechanisms to protect and authenticate (where possible) communications between IoT devices within the endpoint eco-system or between endpoints.

For example, if two objects are approaching each other at a known rate, security applications in the Service Ecosystem can prepare session keys specific to these two endpoints before they reach a distance where they can physically impact one another. This would ensure that secure communication between endpoints and IoT sensors within each endpoint can still be used in the event that there is no time to renegotiate an instantaneous secure session when the potential for a critical scenario (like an impending automotive crash) is detected.

Thus, an augmentation to the TCB implementation is required. Two solutions, that enable the UICC to be utilised as a TCB, are described in GSMA document IoT.04 "Common Implementation Guide to Using the SIM as a 'Root of Trust' to Secure IoT Applications" [21]. One solution describes the use of a SIM applet (IoT SAFE) and another the use of Generic Bootstrapping Architecture (GBA).

Another critical issue in these environments is detecting compromised IoT devices within a single endpoint (vehicle). For example, how can the environment recognise whether a simple sensor, such as a Tire Pressure Monitor (TPM) has been compromised? If the other IoT devices within the endpoint make a critical decision based on the compromised TPM signalling a tyre has blown, a safety issue may arise. As a result, the behaviour of devices, and their trustworthiness, must be reassessed at every boot-up phase. All IoT devices within the endpoint eco-system should have tamper resistance and must be able to notify other peer IoT devices within the endpoint eco-system and potentially the manufacturer if there is a compromise. Inversely, there should be a way that other IoT devices in the endpoint ecosystem can evaluate the trustworthiness of peers in the network.

## 12.6 The Result

After implementing the recommendations, the vehicle sensor network is well guarded against attacks on the vehicle communications network. GBA is used to distribute keys to all IoT devices in the system, and does so on every boot-up, ensuring that old keys are not reused. This, along with tamper resistance, a strong TCB in every IoT device, and a manufacturer root of trust, allows the environment to function with far less risk.

Yet, regardless of these changes, safety is still a critical factor. The engineering team and business leadership, along with the company’s legal team and insurance brokers, should evaluate safety critical technology and determine whether security can be implemented without introducing alternate safety risks (e.g., caused by increased communications delay). While security can often be implemented, even in safety-critical scenarios, with some architectural adjustments, there are times when safety or usability must come before all other concerns.

## 12.7 Summary

Systems like these are often well engineered and take a large amount of effort to attack the ecosystem. However, subtle flaws in the communications architecture can lead to a compromised environment. In walled gardens, such as some CANbus networks, a single flawed IoT device with the endpoint eco-system can cause the entire endpoint system to become vulnerable. This, in safety-critical environments, is unacceptable.

# Annex A Regulatory Aspects Associated with IoT Services (Informative)

A defining characteristic of many IoT services is the vast collection of personal data such as user location, user activity and healthcare data. Importantly, in the case of many IoT services, objects and services must be connected to one another and share data about a specific user in order to be seamless and function properly.

With the use of identity and identification technologies, the ability to consistently and uniquely identify objects and users to ensure communication with the devices has significant implications to the privacy of data subjects. At the same time, the use of identity and identity management technologies, by ensuring that appropriate access control mechanisms are in place, also provide good opportunities to enable privacy enhancing frameworks.

In this respect, identity verification, authentication and authorisation standards provide access control solutions for both the users and things (devices). For example, role-based access control could include mechanisms where certain actions can only be associated to a specific role (e.g. collection, transmission or processing of data) with permission frameworks managed by administrators (or the users themselves) in order to protect privacy and user’s preferences.

IoT privacy considerations need to be made across multiple key layers of hardware, communication (network) and application layer, and taken into account by chip manufacturers, device manufacturers, software and application developers, communications network operators and the IoT Service Providers.

## A.1 GSMA IoT Privacy by Design Decision Tree

In order to build trust in the IoT ecosystem and minimise the need for formal regulatory intervention, the GSMA proposes the following high-level steps as a guide to minimising any privacy risks. We recommend that IoT Service Providers follow these steps and consider these questions at the early development stages of their IoT service or product. Sections A.3 to A.6 in this annex provide information to be considered when following these steps.

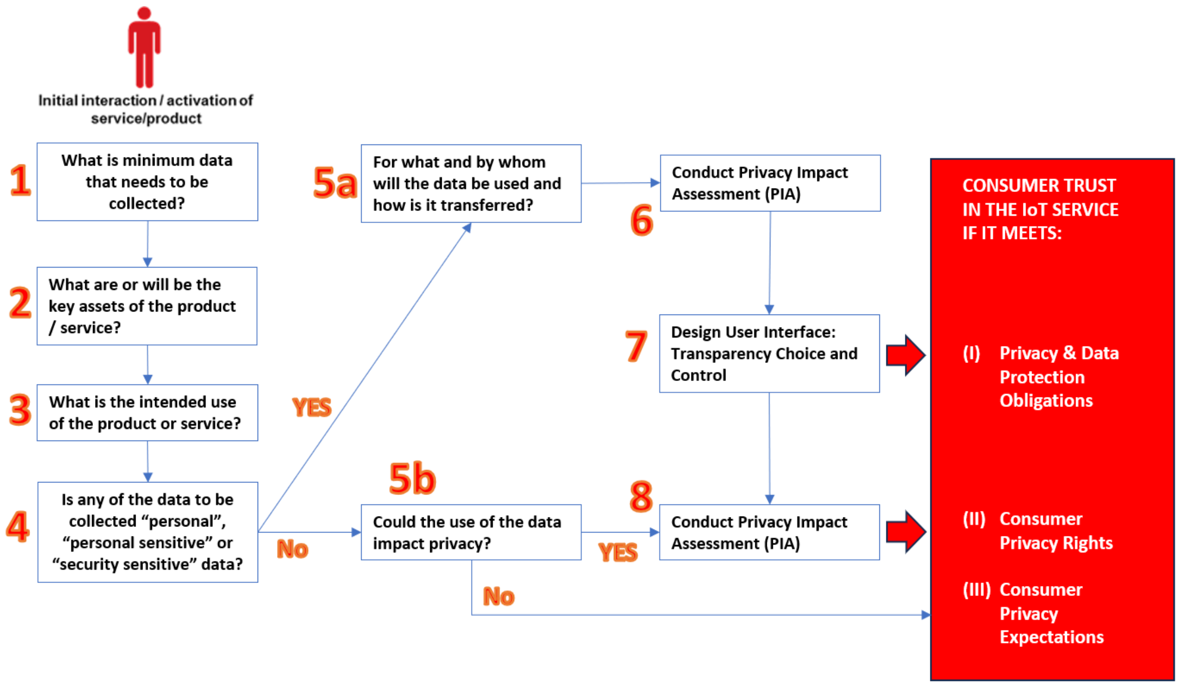
Initial interaction / activation of service/product
1
What is minimum data that needs to be collected?
2
What are or will be the key assets of the product / service?
3
What is the intended use of the product or service?
4
Is any of the data to be collected "personal", "personal sensitive" or "security sensitive" data?
YES
No
5a
For what and by whom will the data be used and how is it transferred?
5b
Could the use of the data impact privacy?
YES
No
6
Conduct Privacy Impact Assessment (PIA)
7
Design User Interface: Transparency Choice and Control
8
Conduct Privacy Impact Assessment (PIA)
CONSUMER TRUST IN THE IoT SERVICE IF IT MEETS:
(I) Privacy & Data Protection Obligations
(II) Consumer Privacy Rights
(III) Consumer Privacy Expectations

**Figure 12 – GSMA IoT Privacy by Design Decision Tree**

| Step | Consideration |
|---|---|
| Step 1 | **What is the minimum data that needs to be collected from / about the user so that your IoT service or product can function properly?**<br>One of the first steps in any business model relying on data is to identify the minimum information that is actually required from or about the consumer, for the service or product to function properly. The types of data a service requires could be categorised as static – such as the consumer's name or home address – and data that is dynamic, such as real-time location.<br>So, if you are offering, for example, a fitness wristband tracking someone's steps and calories burned, then you would need to know the weight, age, gender, distance travelled and the heart rate of the individual wearing the wristband, but you would arguably not need the actual location of the individual.<br>When assessing the types of data needed, it's also important to decide whether the individuals' consent is needed to use that data and how you would obtain their consent or indeed offer them options to control their privacy preferences. A smartphone could act as a medium for offering the user privacy options (e.g. mobile app or online dashboard) where the product itself has no screen.<br>In all cases only the minimum data needed should be collected and that data should only be collected, transmitted, stored or processed for as short a period of time as possible (except as required to meet statutory regulatory requirements).<br>Any data which may optionally be collected should only be collected if the user opts in to collection and processing of additional optional data.<br>Users should not be opted in by default for collection, processing or storage of any data above the absolute minimum required for the basic product or service to function. They |

| Step | Consideration |
|---|---|
| | need to be offered the option to "Opt In" with a clear explanation of the purpose for which and by whom this additional data will be used and must be able to "Opt Out" again any at any time. |
| Step 2 | **What are or will be the key assets of the product / service?**<br>Having identified the minimum data that is needed for the product / service in step 1, it is necessary to consider where data or security sensitive information is generated, stored, transmitted or processed. This list of interfaces, subcomponents, hardware and software will help the designer identify which specific elements of a product or service need specific security mechanism to be applied. |
| Step 3 | **What is the intended use of a product or service?**<br>While most IoT products or services will not be part of a nuclear power station, many IoT device will handle privacy related or financially valuable information that is attractive to attackers. It is therefore necessary to consider the intended use and threat landscape within which a product or service will be used.<br>This included whether the product or service will be used in a largely standalone manner or whether it will be part of a larger IoT system, network or deployment. This will need to include consideration of both remote attacks and whose where an attacker may be able to gain physical assess to the product or service for a period of time.<br>Security mechanisms need to be proportionate to the expected threats and types of attackers that the product or service will be exposed to in its expected deployment environment. |
| Step 4 | **Is any of the data to be collected "personal", "personal sensitive" or "security sensitive"?**<br>The data or information collected by a single IoT product or service can be of varying levels of sensitivity. It is therefore necessary to identify the types and sensitivity of all data that is to be stored, transmitted, processed or stored within the product or service. The security mechanisms applied to each type of data or information need to be appropriate to sensitivity of that data or information.<br>While some data may not in itself be personal data that leads to a direct privacy risk, lower sensitivity data may allow identification of a user by inference or association over a longer period of time and therefore such data may need to be handled as if it was personal data.<br>Similarly, security sensitive information such as cryptographic keys, passwords, or network assess credentials may provide an attacker with an indirect path to compromise of user privacy and therefore need to be protected appropriately. |
| Step 5a | **For what and by whom will data be used and how will it be transferred?**<br>Once you have established what data needs to be protected and security environment in which it needs to be protected, the next step is to map out how the data you collect will be used – and who they need to be shared with – to achieve intended outcomes as part of your service offering. The following questions should help you address both security and privacy considerations in relation to the treatment of the data:<br>• Is the data kept secure both when stored and transmitted?<br>• Have you clearly set out the data flows? I.e. identify how the data will be used and shared across the value chain and for what purposes. |

| Step | Consideration |
|---|---|
| | • Can you justify why each type of data collected is needed in the specific context of offering the intended service?<br>• Have you defined/agreed privacy responsibilities with your partners from the outset (and does your product design reflect these responsibilities?)<br>• Are there appropriate contractual agreements in place with the companies you are sharing consumers' data with? (E.g. limiting the use of data by analytics providers for their own commercial purposes). Such agreements or restrictions can be bilateral or you could establish a code of conduct or guidelines and ask your partners to commit to them with defined consequences and liabilities if they fail to do so.<br>• How long each data type needs to be kept at each point within a product or system and identify how the data will be deleted once it is no longer required or permitted to be retained. Data should not be kept longer than absolutely necessary.<br><br>**How is personal data regulated in law?**<br>Data protection regulations (e.g. EU GDPR [16]) are now largely uniformly applicable in all countries. While there are variations, basic data protection regulations will apply to all IoT products regardless of eventual country of use. However, there are some local specific regulatory aspects that need to be considered:<br>• What is the definition of 'personal' data in the country/market concerned?<br>o Are there any sub classes of more sensitive data?<br>• What is the legal basis for collecting or retaining each type of data?<br>• Are there any specific restrictions on what can be collected or retained, including any restriction on maximum duration?<br>• Are you subject to any privacy-related licence conditions (e.g. as a telecoms provider)<br>• Are there any federal, state, local or sector-specific laws that apply in relation to your proposed data collection model, in addition to general data protection laws? e.g.:<br>o Financial / payment services, healthcare regulations<br>• Are there any restrictions on where data can be stored, processed or transferred.<br>o Potential restrictions on cross-border data transfers.<br>• Are the security mechanism needed to protect or secure data subject to export restrictions such as Wassenaar [32]. |
| Step 5b | **Could the use of data impact an individual's privacy?**<br>Your product or service may collect data that is not necessarily classified as 'personal' in law but may still have privacy implications to the consumer. To ascertain whether the relevant data could impact a consumer's privacy consider the following:<br>• Could (non-personal) data from your service/product be combined with other data from different sources to draw inferences about the consumer? For example, inferences about his/her lifestyle, habits or religion that may:<br>o Allow identification or tracking of the consumer?<br>o Be used by 3rd parties (retailers, insurance companies) to track or discriminate against the specific consumer?<br>• If your product or service is likely to change at any point in the future what are the likely privacy implications of any such change on the consumer. For example: |

| Step | Consideration |
|---|---|
| | ○ Does the change involve the collection of new data about the consumer (such as location data)?<br>○ Is there any data previously collected that is no longer required and therefore should no longer be collected, processed or stored.<br>○ Are existing or new consumer data shared or sold to third parties (e.g. advertisers) who would start using consumer data for different purposes than those originally obtained for?<br>• If any such changes occur, you should:<br>○ Check the possible impact on your business if new laws are invoked as a result of the change.<br>○ Establish processes to inform the consumers and obtain their consent where necessary.<br>○ Provide the means for consumers to change their privacy preferences at any time.<br>• Some additional considerations that we recommend IoT service providers consider are:<br>○ Make sure you have appropriate contractual agreements in place defining the responsibilities of each partner in the value chain when collecting, processing or storing data.<br>○ Have a clear process of redress so that the consumers know who to turn to if things go wrong or if they suffer from a privacy breach. |
| Step 6 | **Conduct a Privacy Impact Assessment**<br>Conducting a Privacy Impact Assessment (PIA) is about:<br>• Identifying what, if any privacy risks your product or service raises for individuals.<br>• Reducing the risk of harm to individuals that might arise from the possible misuse of their personal information.<br>• Designing a more efficient and effective process for handling data about individuals.<br>PIA requirements are increasingly becoming common in data protection and privacy laws. There are a number of guides on how to conduct a PIA including those published by the UK's Information Commissioner's Office [9], [31] and those by the International Association of Privacy Professionals.<br>Typical questions to be addressed when conducting a PIA include:<br>• Will the project result in you/your partners making decisions or taking action against individuals in ways that can have a significant privacy impact on them?<br>• Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, sensitive personal data, health records, criminal records or other information that people would consider to be private?<br>Will the product or service require you to contact individuals in ways that they may find intrusive?<br>For how long and where does data need to be stored? |

| Step | Consideration |
|---|---|
| | How will data be deleted when it is no longer permitted to be retained (any data to be collected, processed, transmitted or stored must have both an explicit purpose and maximum duration)?<br>How will deletion of any personal data in any backups or across multiple products or services be handled?<br>If a user exercises their “right to me forgotten” (e.g. under GDPR [16]), how will this be achieved? |
| Step 7 | **Design Privacy into the User Interface**<br>After assessing the privacy risks to the consumers, you should consider how to raise those consumers’ awareness of such risks and how to mitigate them as well as offer them options to express their privacy preferences at any time.<br>Ultimately, this step is about ensuring you offer a service that meets your legal obligations and the consumers’ needs and expectations in a user-friendly way. And it’s about building their trust by reassuring them that they have more control over their privacy. Questions to consider include:<br>• How can consumers be made aware of any risks to their privacy and how can they make informed choices?<br>• Have you obtained their consent, where legally required?  Key elements of consent include: disclosure, comprehension, voluntariness, competence, and agreement)<br>• Is data secured in transit and at rest?<br>• Is there a set period for which you need to keep consumer data (and why)?<br>• Does the consumer journey help gain their trust? For example:<br>o Do they understand what data they are sharing in return for using the service?<br>Can consumers express their privacy preferences in simple steps e.g. via a web based ‘permissions dashboard’, ‘just-in-time’ prompts, a call centre, a mobile app, a voice activated command etc. |
| Step 8 | Following step 7 (if applicable), elements of the step 6 PIA will need to be revised to ensure the privacy is still adequately addressed. |

## A.2 Privacy Overview

Key design considerations are influenced by law [13] and consumer attitudes and concerns [14], [15].  The latter may be sectoral specific, such as for connected toys and children’s privacy and safety or for IoT enabled healthcare services. Key considerations include:

### A.2.1 Transparency, Notice and Control

Data protection laws such as the EU GDPR mandate that organisations must be transparent and provide individuals with a range of information about how their data will be used and requires them to process data fairly and in accordance with key rights that give individuals specific control over their data.

The IoT and smart connectivity is by its nature, seamless and ubiquitous involving the broadcast of data and allowing its observation and collection in real-time simultaneously between multiple parties, often across borders.  The requirement for transparency and control, demands an approach beyond a burdensome privacy policy. Providing notice and behavioural nudges that are contextual and fine grained which allows people to choose what personal data and attributes they wish to share, with whom they share it, the purposes, duration etc. (see section A.2.1 on data protection and privacy by design and default).

Data collection, processing or storage about the minimum necessary to provide the basic product or service must be on the principle of “Opt In”, with an easy means for the user to change their mind and “Opt Out” at any time.

In many countries a citizen has the right to request a copy of all data held by a company about them. Where the data privacy regulations require this, companies must provide a published point of contact and have procedures in place to handle such requests within the time limits defined in the applicable regulation.

### A.2.2 User access to privacy controls.

Not all IoT devices provide a graphical, keypad or other complex user interface which allows users IoT to review or change privacy setting of the product or service. Where simple user control of privacy options cannot be built into the product or it is more practical to manage these at a service level,

Privacy regulations (e.g. GDPR) require the purpose for which any collection, processing or storage of personal data to be clearly communicated to users. Data controllers are required to inform data subjects about intended data processing purposes, contact details of the data controller, the recipients of the subject’s personal data, the period for which the personal data will be stored, the usage of profiling, and the existence of automated decision-making, including profiling. Information about the intended processing purposes can be conveyed using standardised icons alongside short texts.

In all cases the user must be “Opted Out” by default and must “Opt In” to any data collection, processing or storage for all purpose above that which is required to provide the basic product or service. The use of all data including any data that is “strictly necessary” for the purpose of providing the service must be explained to the user before they are given the option to opt in.

Except where the minimum collection of strictly necessary personal data is linked to a service contract that a user has signed in advance (e.g. collection of personal data required as part of a mobile network contract and subsequent processing or storage by the network), it may be necessary to require the user to “opt in" to all data processing, including strictly necessary data when using a product or service for the first time.

Where not provided at a product level or where it is more practical to control privacy setting across multiple products, control of privacy options needs to be provided at a service level. In such cases the service needs to provide a simple API, webpage or portal through which the user can review and control the collection, processing and storage of personal data associated with the product(s) and service(s).

The IoT service must provide as a minimum the following rights in relation to data collected:

- the right to have data erased (except where required by other regulations -e.g. financial);

- the right to have data corrected;
- the right to restrict the processing of data; and
- the right to obtain a copy of personal data.

### A.2.3 Subscriber vs. User

A key challenge in the mobile sector is differentiating between a subscriber who may be a company or parent and the end user of a device who may be the employee or child. In the EU, in addition to the GDPR, separate ePrivacy rules restrict the use of data and give rights to subscribers and end users, and to legal persons. This creates design challenges for transparency, control and rights and for identity management (and identity attributes).

Similarly, some devices may be shared between multiple parties within a group of people (e.g. a family or employee group) or the device may be rented to unrelated persons for a fixed period of time (e.g., the vehicle example in this guide). It is necessary to consider privacy impacts, data isolation and data deletion in all these scenarios if applicable to your product or service.

## A.3 Data Protection Overview

Crucial to IoT services is the adoption of Data Protection and Privacy by Design and Default (DPPDD). Data protection and privacy must be embedded from the outset. DPPDD is now mandated by the GDPR.

### A.3.1 Data Protection and Privacy by Design and Default

DPPDD requires organisations to consider the “nature, scope, context and purposes of processing” and the risks to individuals, and to adopt both technical and organisational measures to integrate safeguards and protect the rights of individuals. Some of the measures mandated by the GDPR include includes adopting privacy enhancing techniques such as:

- Data minimisation: ensuring by default, that only “personal data which are necessary for each specific purpose are processed.” This “applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility”.
- Ensuring by default that “personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.” This clearly requires robust identity and access controls.
- Pseudonymous and anonymous connectivity and use of services.
- Use of encryption.

DPPDD provides network operators and other key stakeholders with an opportunity to build services that foster trust and confidence in IoT services.

Consideration should also be given to the need to design services so individuals can access these services in ways that are not linkable and that allow individuals to be free from observation (for example, when the use of data is not necessary to connecting a service or authenticating a device or person). Concerns over being observed and tracked online act as a barrier to economic activity.

### A.3.2 Data Protection Impact Assessments

Data Protection Impact Assessments are now required by some laws such as the GDPR where processing is likely to result in high risks to the rights and freedoms of individuals. Some of the broader freedoms that might be impacted by IoT enabled smart services are the right to freedom of association and movement for example, and the right to a private life. A DPIA helps organisations systematically and comprehensively analyse the intended processing and to identity and mitigate risks.

DPIA may also help data subjects to better understand the possible risks of their usage of an IoT service, and to freely consent to data processing. Greater communication of risks can help increase trust in IoT services.

### A.3.3 Codes of Conduct

Data protection laws may require key sectors or associations to create Codes of Conduct. Codes of Conduct can help organisations particularise high-level principles and apply data protection law in affective manner.

For example, one of the most pressing problems concerning many new connected services is discrimination (see recital 39 of the EU GDPR [16]). Tools such as ethical algorithmic auditing should be implemented to flag up discrimination. Internal auditing schemes could also be considered to guard against discrimination of protected groups, but also to protect victims of unanticipated discrimination.

## A.4 Data Protection and Privacy Assessment

It is estimated at the end of 2023 that around two thirds of the world population will be covered by EU GDPR equivalent data protection laws [13]. These laws establish a common set of core *Principles* that set out conditions and obligations over the use of peoples' personal data, that provide individuals with key rights, and that seek to make organisations open and accountable about their use of such data. As these laws are revised and new laws come about, we find 'data protection (and privacy) *by design* and *default'* [17] emerge as a legal requirement, from the EU's General Data Protection Regulation (GDPR) [16] and the Council of Europe's Convention 108+ [18], to India's data protection bill [19]. Some of these laws may also expressly require organisations to offer anonymous or pseudonymous access to services and processing of data.

These legal developments are already shaping the design of IoT services by virtue that they:

- may class device identifiers, online Identifiers or a person's social identity as 'personal data';
- expressly require that organisations consider the risks to individuals through the processing their personal data;
- impose significant penalties for failing to adopt data protection by design and default and for failing to take appropriate measures to guard against the unauthorised access to or disclosure of personal data;
- require that by default, personal data is not made accessible without an individual's intervention to an *indefinite number of natural persons* – this GDPR requirement has particular implications for IoT services.

*'Data protection by design'* means considering and implementing measures to safeguard the privacy and data of individuals, from concept to technical specifications, to product or service design through to their operation. An example is the use of pseudonymous Identifiers or the use of encryption to protect against unauthorised access to data or network authentication protocols.

*'Data protection by default'* means that organisations should put the individual first and provide them with effective choices and controls over the use of their personal data, adopt techniques such as data minimisation to ensure only data that is necessary is processed and set privacy-respectful and protective default settings and ensure data isn't accessible to an indefinite number of persons. The concept and legal requirement of 'data protection', 'privacy by design' and 'default' influences greatly the design of IoT user interfaces and user experience.

## A.5 Consideration of General Data Protection and Privacy Principles

Many IoT service-related attributes including a pseudonymous customer reference will be considered personal data under regional and national data protection laws. For example, under the GDPR, personal data is any information that allows a living individual to be identified (either directly *or* indirectly) or that permits a person to be *singled out*. Examples of 'personal data' include (but are not limited to) Identifiers such as a name, an identification number such as a MSISDN/GPSI, IMEI/PEI, IMSI/SUPI, credit card number, passport number, driver's licence number, an email address, location data, or other online Identifiers such as an IP address or MAC address (in context) or a person's social identity.

Data protection laws such as the GDPR or Brazil's General Data Protection Law, may also treat biometric data as more sensitive and subject to additional rules. For example, such data may only be processed where national laws permit it or with an individual's explicit consent. Of note, 'biometric data' may include "*physical, physiological or behavioural characteristics of an individual which allows or confirms the unique identification of that individual*" (See UK Data Protection Act 1998, Section 205 [20]). Clearly, such definitions and will impact on the design and implementation of many IoT services.

Also of note, is that laws such as the GDPR, or those based on Convention 108+ will require organisations deploying IoT services to conduct Data Protection Impact Assessments where they involve the systematic and extensive profiling resulting in high risks to individuals, or that otherwise involve the processing of biometric data or that track an individual's location or behaviour or that profile children for example. In addition to these factors and the key principles outlined below, the design of IoT services should also consider the need for 'un-likability' and 'un-observability' to guard against unauthorised tracking of individuals and insights into their behaviour and any negative impact on their privacy and the security of the authentication processes. Such considerations should form part of the data protection (and privacy) impact assessment.

## A.6 Key Data Protection Principles

Common to key regional and data protection laws are the following principles that the design of IoT Services should consider.

### A.6.1 Fair, Lawful and Transparent Processing

This means processing personal data in ways that are **fair** to individuals, that avoids risks and harm and that meets at least one condition to make processing '**lawful'**.

In practice this means:

- being open about what data you require and why;
- using data in ways individuals would reasonably expect;
- ensuring you have a lawful basis set out in law, such as:
  - where the law requires it; or
  - with the **consent** of individuals (though this should rarely be the case for IoT services); or
  - for entering into/the performance of a **contract** with individuals; or
  - to meet an organisation's legitimate interests such as for fraud prevention or network security purposes (except where an organisations interests are overridden by the interests or rights of individuals).

| Privacy Principle | Privacy by Design Recommendation |
|---|---|
| **PP1 Fair, Lawful and Transparent Processing** | **PDR1.1** Consider how to ensure the use of personal attributes are within the reasonable expectations of individuals.<br>Provide a Short Contextual Privacy Notice at the point at which an individual is asked to use personal data attributes for the purposes of the IoT service, and that notifies the user of:<br>• identity of controller;<br>• data to be processed;<br>• data uses (unless obvious from context);<br>• how to contact the controller, especially regarding how to exercise privacy rights.<br>**PDR1.2** Identify the legal basis for processing personal data (such as it is necessary for performance of a contract to give access to an account and data, or consent).<br>**PDR1.3** If relying on consent, provide granular choices – do not bundle consent – and ensure individuals are aware of the persistency of consent and how to revoke it.<br>**PDR1.4** Capture and retain evidence of consent revocation.<br>**PDR1.5** Identify the legal basis for processing special categories of personal data such as biometrics.<br>**PDR1.7** Assess whether individuals would reasonably expect the intended processing, especially secondary uses of their attributes and credentials, and consider the legal basis for such secondary uses. For example, would a user credential or 'identity' be used to track and profile an individual for purposes not connect with the IoT service, such as gaining insights into product use and targeting of commercial products - if so, then consider the legal basis and whether consent is required (See PDR2.6). |

| Privacy Principle | Privacy by Design Recommendation |
|---|---|
| | **PDR1.8** Identify any legal obligation to provide notices in a specific language or languages.<br>**PDR1.9** Use clear language and text/images appropriate to the target audience and context to ensure the user understands what is being asked of them and what they are agreeing to.<br>**PDR1.10** Place a hyperlink in the short Privacy Notice to the more detailed company Privacy Statement that explains the IoT service in clear simple ways. |

### A.6.2 Purpose and Use Limitations

Personal data should be collected and used for a specified purpose and not used in ways that are incompatible with those purposes.

The purpose and use limitation principle serves two key objectives. The requirement to specify what data will be collected and for what purpose is important to ensuring fair and transparent processing and that is in line with the reasonable expectations of individuals. Secondly, it ensures organisations justify their collection and use of personal data ensuring they have a legal basis for doing so.

| Privacy Principle | Privacy by Design Recommendation |
|---|---|
| **PP2 Purpose and Use Limitations** | **PDR2.1** Allow people to choose the presentation of their identity and only require the presentation of personal identifiers where unavoidable (such as a MSISDN, or name or email address).<br>**PDR2.2** Prevent the unauthorised linking of identifiers and authentication protocols across different services.<br>**PDR2.3** Identity, justify and document the purpose or purposes of data processing (for example, according to a legal requirement or business need).<br>**PDR2.4** Notify the ‘purposes’ if data processing in a privacy notice.<br>**PDR2.5** Limit the collection and use of personal information to that necessary (as opposed to desirable) for the identified purpose.<br>**PDR2.6** Conduct an impact assessment for any secondary uses of data to determine if they are compatible with the original purposes for which they were collected and within the reasonable expectations of individuals and identify a legal basis in data protection law and consider if consent is required for secondary uses (as it will often be).<br>**PDR2.7** Limit the tracking of identifiers or user behaviour to that necessary to provide or protect a service (such as authentication and authorisation). |

### A.6.3 User Choice and Control

It is important that individuals have choice and control over what attributes are obtained, verified and used when establishing IoT service credentials and enabling access to IoT services. A process should be established to ensure individuals can express and revoke consent, for example, or by which they can determine what credentials are created and presented.

| Privacy Principle | Privacy by Design Recommendation |
|---|---|
| **PP3 User Choice and Control** | **PDR3.1** Provide individuals with the opportunity to determine their IoT service 'identity' and the personal data and attributes used in the creation and presentation of such identities.<br>**PDR3.2** To the extent required (or deemed appropriate) seek and obtain the consent of individuals, but at all times ensure fairness and transparency over the use of personal data and attributes for the purposes of the IoT service.<br>**PDR3.3** Provide individuals with the means to associate, disassociate and re-assign their IoT service identities. |

### A.6.4 Data Minimisation, Proportionality and Retention

A key means to help reduce risk and protect privacy is to minimise the data collected and used, including metadata around access to services or use of a service.

In practice this means organisations should only collect sufficient information to fulfil an identified purpose and ensure they don't collect or hold more than is necessary to meet that purpose or purposes.  Data shouldn't be collected or held just because it might come in handy one day – it has to be necessary, proportionate and justified.

These obligations can be met both by identifying the minimum data needed, by setting data retention policies and by giving users the means by which they can delete, add or update data held about them.

| Privacy Principle | Privacy by Design Recommendation |
|---|---|
| **PP4 Data Minimisation and Retention** | **PDR4.1** To minimise the risk of compromise to personal data and an individual's privacy, the collection and use of personal data (especially personal identifiers) for the purposes of identification, authentication and authorisation should be avoided. Consider the use of pseudonymous identifiers to protect the privacy of individuals.<br>**PDR4.2** Provide individuals with choices and control over what data is provided, including the presentation of their identities.<br>**PDR4.3** Prevent or restrict unauthorised entities from observing and collecting personal data and metadata relating to the use of the IoT service credentials.<br>**PDR4.4** Identify the minimum attributes needed to meet a specific IoT use case. This should consider the type, sensitivity and granularity of the attributes, volume, frequency of collection, and metadata generation.<br>**PDR4.5** Set a data retention policy specifying the period for which personal information should be retained, including log files. This should reflect local law.<br>**PDR4.6** Ensure data is securely deleted when no longer required, including log files. |

| | |
|---|---|
| | **PDR4.7** Establish system and procedural controls to monitor and ensure only the minimum data necessary is processed and that consent is obtained for any additional data processing.<br>**PDR4.8** Adopt privacy enhancing techniques, such as using attributes that presents the value of an atomic attribute in an alternate form (e.g. reducing granularity to protect privacy) or compute a value based on the values of two or more atomic attributes:<br>e.g. DOB -> over 18yrs (Y/N)<br>e.g. Location (Lat/Long) -> Place/POI |

### A.6.5 Data Quality

Poor quality data and data governance measures may pose risks and harm to individuals. It is important to ensure that the personal data and attributes used in IoT services are accurate, complete, reliable and where necessary kept up to date and relate to the correct individual. It is important to ensure that not only is an ‘identity’ correctly associated with a service or device for IoT service purposes, but that such identities can be disassociated – see PDR5.5 below.

This means establishing practices to ensure the quality and verifying the reliability of information during collection and subsequent processing, including ways for individuals to update and correct their information. It is essential to always consider “Is the data fit for purpose? “

| Privacy Principle | Privacy by Design Recommendation |
|---|---|
| **PP5 Data Quality** | **PDR5.1** Establish system and procedural controls to verify and maintain the accuracy and reliability of personal data and attributes.<br>**PDR5.2** Establish system and procedural controls to capture and address data corruptions and mismatches.<br>**PDR5.3** Establish a process (free of charge) by which users can update their information and correct any inaccuracies.<br>**PDR5.4** Verify the validity and correctness of the claims made by the individual prior to making any changes to the personal information, to ensure they are authorised to make such changes.<br>**PDR5.5** Create a process not only to allow individuals to associate their identity with a service or device, but also to disassociate their identity from a service or device, including requests from authorised parties to re-assign identities. For example, an individual selling a home may need to reassign access to a smart thermostat or smart meter or smart fridge or other embedded smart device in the home. |

### A.6.6 Individual Participation and User Rights

To ensure openness and strengthen confidence and trust it is important to ensure users can express their preference and choice over how their data are used and that they can exercise their rights assigned by law or business policy.

| Privacy Principle | Privacy by Design Recommendation |
|---|---|
| **PP6 Individual Participation and User Rights** | **PDR6.1** Ensure privacy notices and longer statements (or policies) explain (in clear language) any privacy defaults, settings and permissions and how to change or set them.<br>**PDR6.2** Ensure privacy notices explain (in clear language) how an individual can contact the organisation with queries or issues regarding the user’s rights.<br>**PDR6.3** Establish procedural and system processes for individuals to obtain a copy of their personal information and how to correct or update their information.<br>**PDR6.4** Establish procedural and system processes by to manage disputes over user requests to update or correct their information. |

### A.6.7 Information Security

There is no one size fits all to information security.  Organisations should adopt a risk-based approach and implement reasonable organisational and technical measures that are appropriate in all the given circumstances to the likelihood and severity of risks to individuals.  A key objective is to prevent personal data and the privacy of individuals from being deliberately or accidentally compromised.  No action should be required on the part of the individual to ensure their data are safe during the data lifecycle. Data must be secure at rest and in transit.

Good security is essential to ensuring the integrity, confidentiality and availability of personal information.  Measures must be taken to protect personal information against unauthorised access, destruction, use, modification, disclosure or loss.

| Privacy Principle | Privacy by Design Recommendation |
|---|---|
| **PP7 Information Security** | **PDR7.1** Document the security measures to be adopted through the data lifecycle.<br>**PDR7.2** Assign responsibility to an appropriate person for monitoring and ensuring compliance.<br>**PDR7.3** Ensure data is transferred securely between all parties involved in the verification or sharing of personal data and attributes. The security should be commensurate to the risks associated with the data types and sensitivity, potential for harm and impact on the user if the data is compromised, and any local regulatory or legal requirement. |

| | |
|---|---|
| | **PDR7.4** Use appropriate access controls to limit access to attribute databases and attribute sources to authorised persons.<br>**PDR7.5** If using third parties to process information on the controller's behalf, the controller must ensure such 'data processors' adopt appropriate and equivalent security measures. |

### A.6.8 Accountability

The principle of 'accountability' is gaining in importance and is included in privacy and data protection laws and standards around the world. In data protection terms, 'accountability' is generally regarded as the commitment to, and acceptance of, responsibility for protecting personal data in compliance with laws or other standards. Accountability also refers to the ability of an organisation to demonstrate its compliance with such laws and related promises – "say what you do and do what you say."

| Privacy Principle | Privacy by Design Recommendation |
|---|---|
| **PP8 Accountability** | **PDR8.1** Nominate a person to be responsible for ensuring compliance with appropriate policies, laws and regulations.  You can't just hope things will work out and harm will never materialise.<br>**PDR8.2** Establish an internal compliance programme, policies, procedures and practices, to ensure compliance and on-going oversight and redress for the remediation of non-compliances and identified privacy risks.<br>**PDR8.3** Provide mechanisms for users to report problems and establish systems and procedures to record, investigate and resolve reported problems. |

# Annex B Document Management

## B.1 Document History

| Version | Date | Brief Description of Change | Approval Authority | Editor / Company |
|---|---|---|---|---|
| 1.0 | 26 Apr 2024 | Updated FASG edition of IoT Security Guidelines CLP.11 published by GSMA Connected Living programme 2016-2020. | TG | Alex Leadbeater, GSMA & FASG Device Security Group (DSG) members |

## B.2 Other Information

| Type | Description |
|---|---|
| Document Owner | FASG DSG |
| Editor / Company | Alex Leadbeater - GSMA |

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at prd@gsma.com

Your comments or suggestions & questions are always welcome.